

FIG. 1

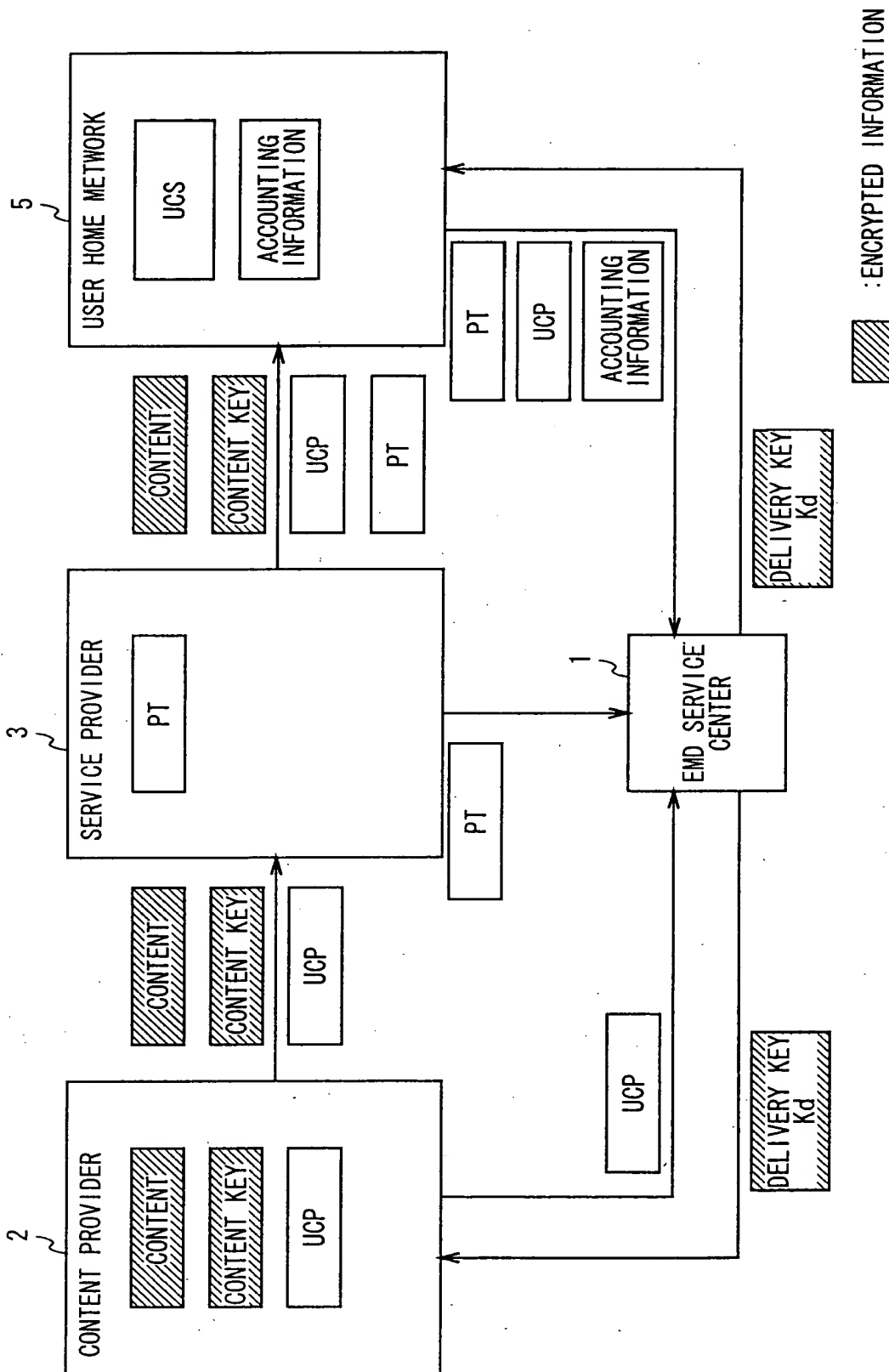
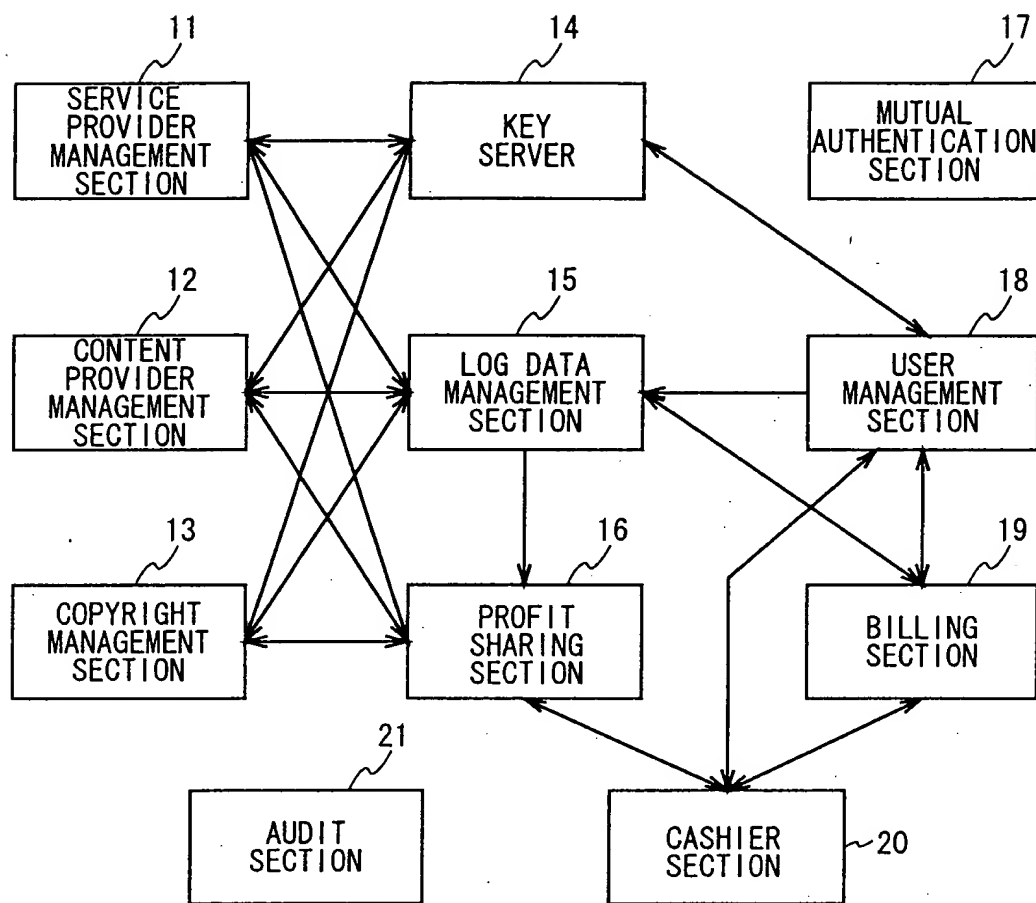


FIG. 2



EMD SERVICE CENTER 1

FIG. 3



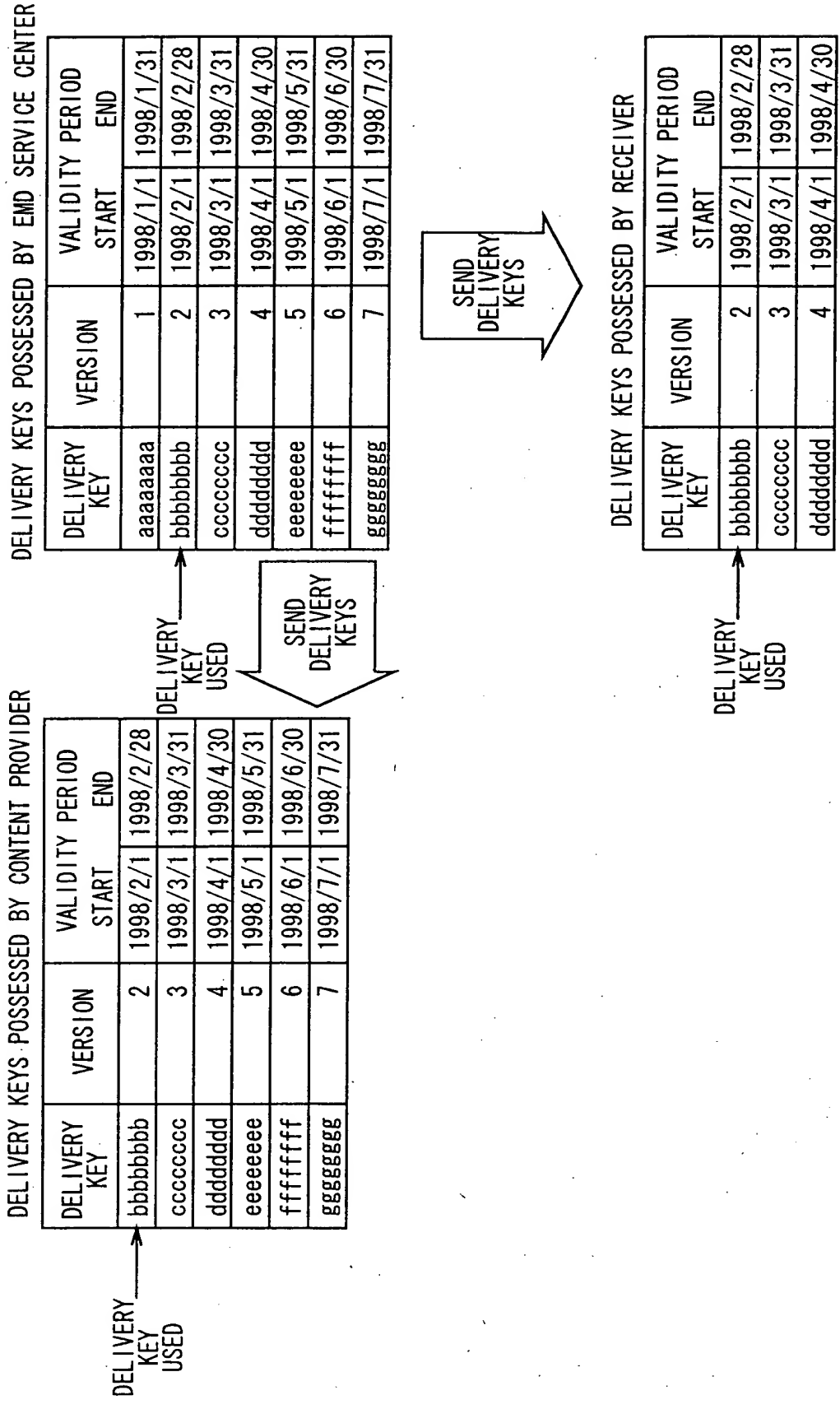


FIG. 5

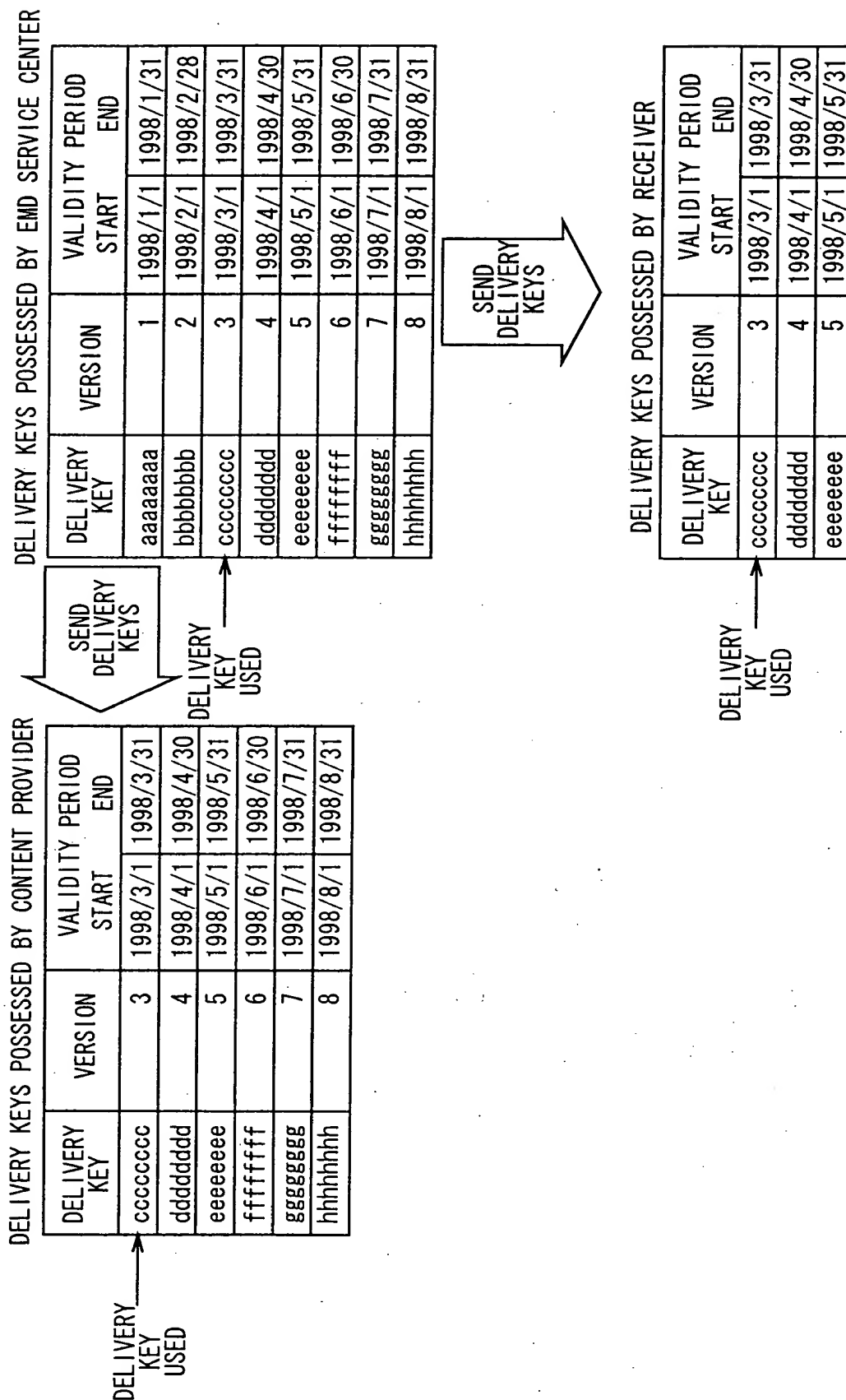


FIG. 6

SECRET

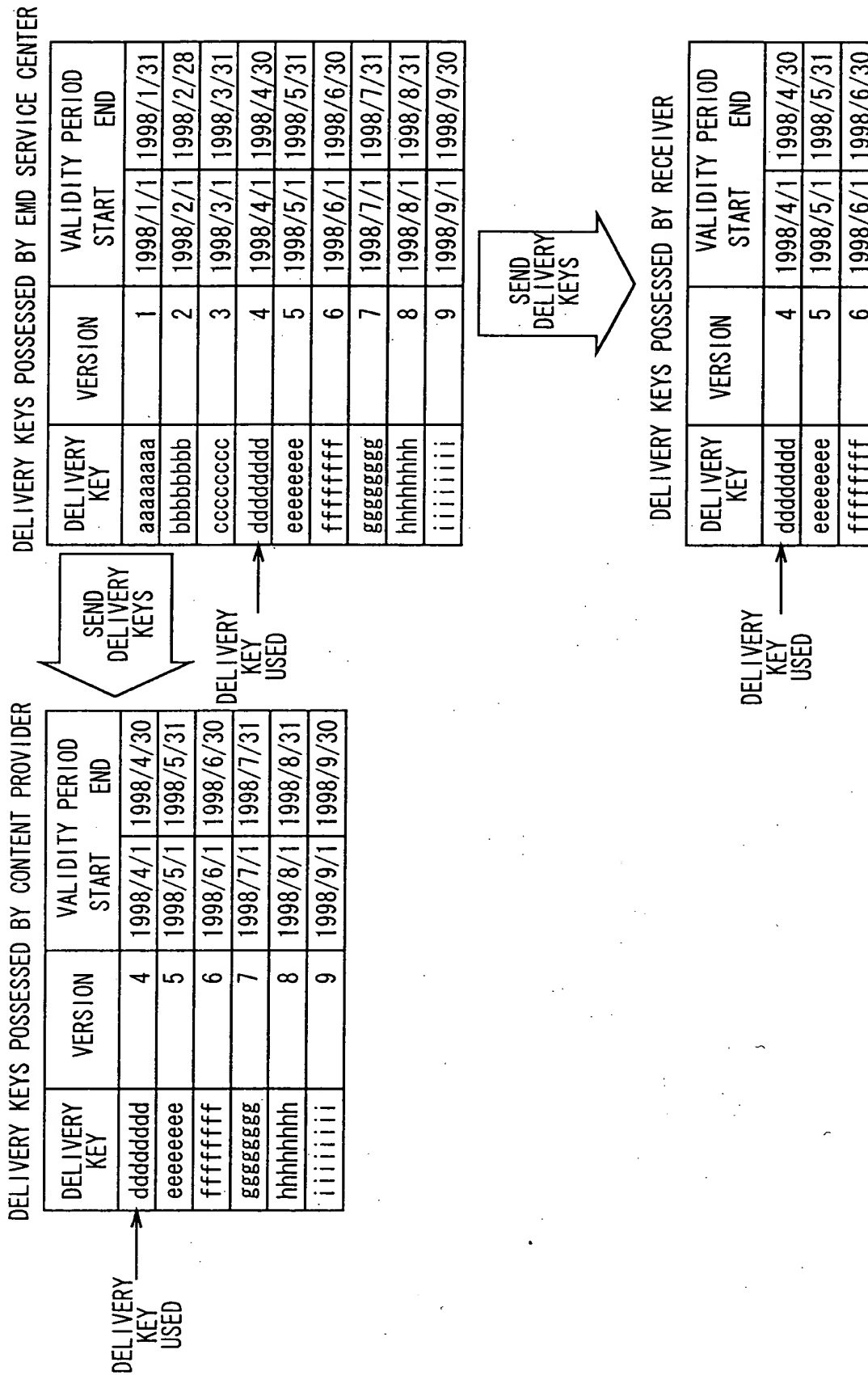


FIG. 7

SAM ID		ID OF SAM62	ID OF SAM212	ID OF SAM311
EQUIPMENT NUMBER		EQUIPMENT NUMBER (100) OF RECEIVERS 51	EQUIPMENT NUMBER (100) OF RECEIVERS 201	EQUIPMENT NUMBER (25) OF RECEIVERS 301
SETTLEMENT ID		SETTLEMENT NUMBER	SETTLEMENT NUMBER	SETTLEMENT NUMBER
ACCOUNT-SETTLING USER INFORMATION	NAME	NAME OF USER F	NAME OF USER F	NAME OF USER F
	ADDRESS	ADDRESS OF USER F	ADDRESS OF USER F	ADDRESS OF USER F
	PHONE NUMBER	PHONE NUMBER OF USER F	PHONE NUMBER OF USER F	PHONE NUMBER OF USER F
	SETTLEMENT INSTITUTION INFORMATION	SETTLEMENT INSTITUTION INFORMATION OF USER F	SETTLEMENT INSTITUTION INFORMATION OF USER F	SETTLEMENT INSTITUTION INFORMATION OF USER F
	DATE OF BIRTH	DATE OF BIRTH OF USER F	DATE OF BIRTH OF USER F	DATE OF BIRTH OF USER F
	AGE	AGE OF USER F	AGE OF USER F	AGE OF USER F
	SEX	SEX OF USER F	SEX OF USER F	SEX OF USER F
	USER ID	USER ID OF USER F	USER ID OF USER F	USER ID OF USER F
	PASSWORD	PASSWORD OF USER F	PASSWORD OF USER F	PASSWORD OF USER F
SUBORDINATE USER INFORMATION	NAME		NAME OF USER A	NAME OF USER A
	ADDRESS		ADDRESS OF USER A	ADDRESS OF USER A
	PHONE NUMBER		PHONE NUMBER OF USER A	PHONE NUMBER OF USER A
	DATE OF BIRTH		DATE OF BIRTH OF USER A	DATE OF BIRTH OF USER A
	SEX		SEX OF USER A	SEX OF USER A
	USER ID		USER ID OF USER A	USER ID OF USER A
	PASSWORD		PASSWORD OF USER A	PASSWORD OF USER A

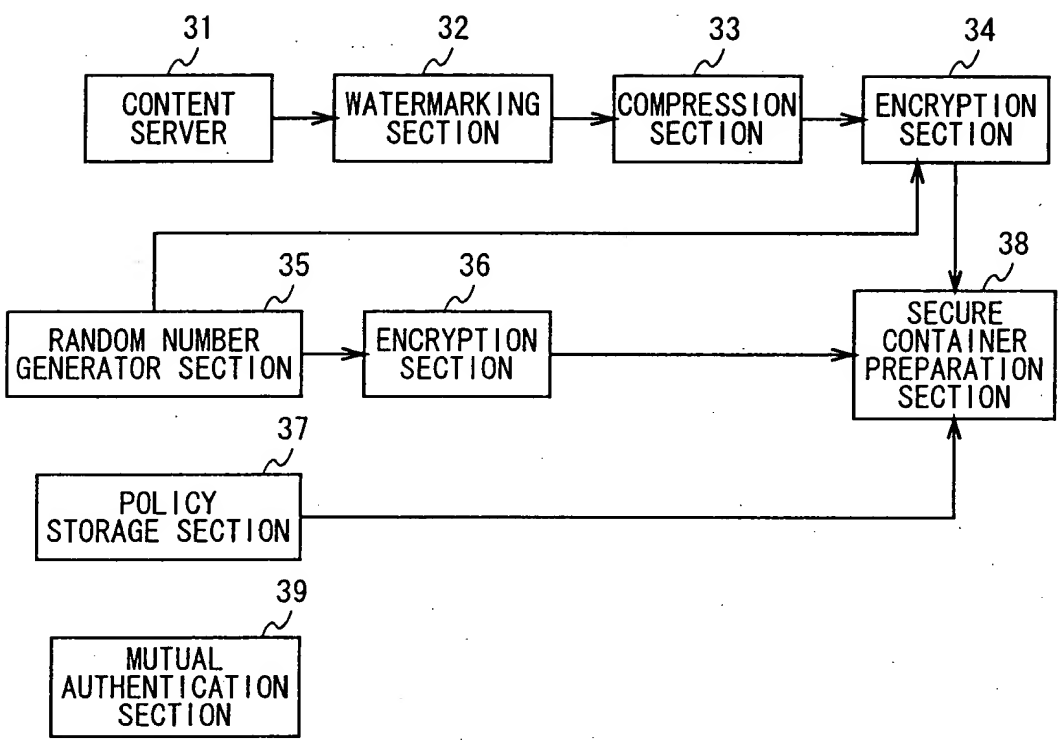
⋮

USE POINT INFORMATION	USE POINT INFORMATION OF RECEIVERS 51	USE POINT INFORMATION OF RECEIVERS 201	USE POINT INFORMATION OF RECEIVER 301
-----------------------	---------------------------------------	--	---------------------------------------

SYSTEM REGISTRATION INFORMATION

FIG. 8

FIG. 9



CONTENT PROVIDER 2

FIG. 9

CONTENT ID	ID OF CONTENT A	
CONTENT PROVIDER ID	ID OF CONTENT PROVIDER 2	
UCP ID	ID OF UCPA	
UCP VALIDITY PERIOD	VALIDITY PERIOD OF UCPA	
USAGE CONDITIONS 10	USER CONDITIONS 10	200 POINTS OR HIGHER
	EQUIPMENT CONDITIONS 10	NO CONDITION
USAGE CONDITIONS 11	ID 11	ID OF USAGE DETAILS 11
	TYPE 11	PURCHASE AND REPRODUCE
	PARAMETER 11	x x x x
	CONTROL TRANSFER PERMISSION INFORMATION	PERMITTED
USAGE DETAILS 12	ID 12	ID OF USAGE DETAILS 12
	TYPE 12	FIRST-GENERATION DUPLICATE
	PARAMETER 12	x x x x
	CONTROL TRANSFER PERMISSION INFORMATION	PERMITTED
USAGE DETAILS 13	ID 13	ID OF USAGE DETAILS 13
	TYPE 13	LIMITED-TIME REPRODUCTION
	PARAMETER 13	x x x x
	CONTROL TRANSFER PERMISSION INFORMATION	PERMITTED
USAGE DETAILS 14	ID 14	ID OF USAGE DETAILS 14
	TYPE 14	Pay Per Copy N
	PARAMETER 14	N TIMES
	CONTROL TRANSFER PERMISSION INFORMATION	NOT PERMITTED
USAGE DETAILS 15	ID 15	ID OF USAGE DETAILS 15
	TYPE 15	TYPE 13→TYPE 11
	PARAMETER	x x x
	CONTROL TRANSFER PERMISSION INFORMATION	PERMITTED
USAGE DETAILS 16	ID 16	ID OF USAGE DETAILS 16
	TYPE 16	TYPE 11→TYPE 11
	PARAMETER	x x x
	CONTROL TRANSFER PERMISSION INFORMATION	PERMITTED

UCPA

FIG. 10

FIG. 11

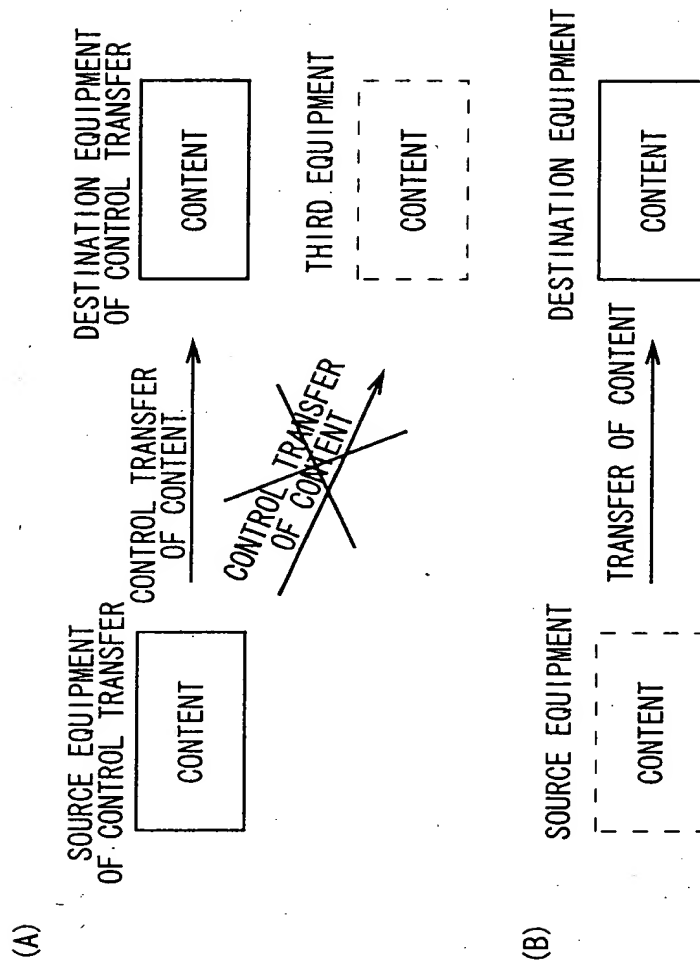


FIG. 11

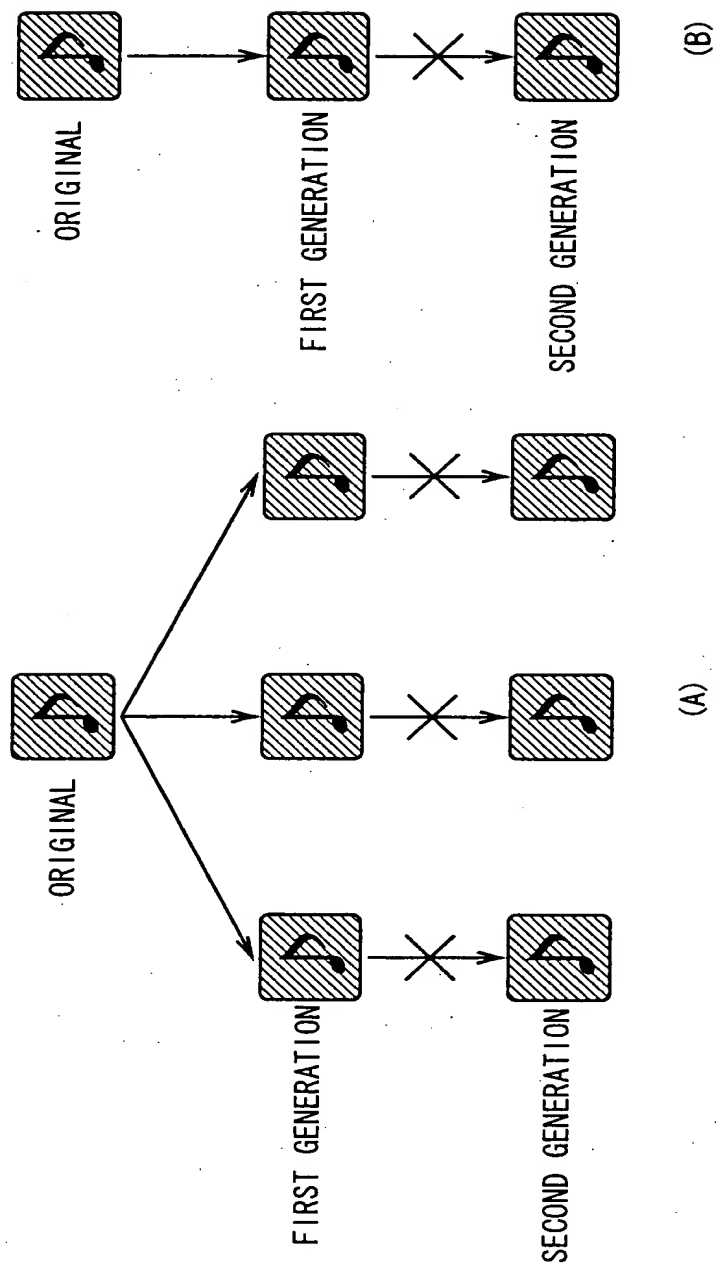


FIG. 12

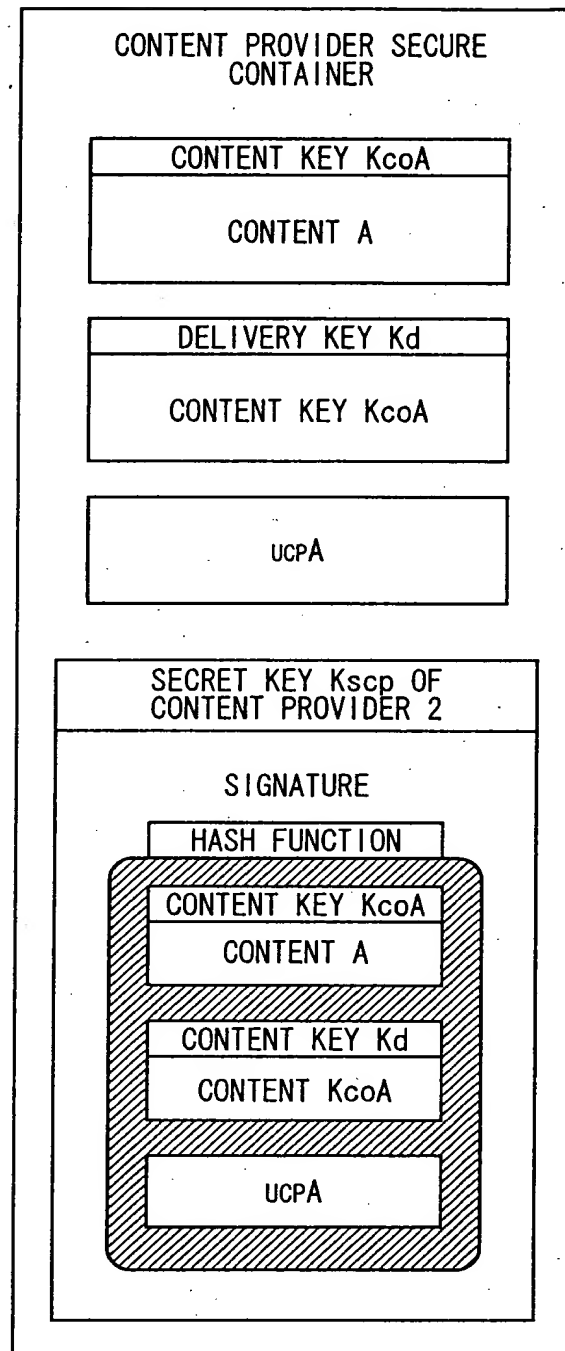


FIG. 13

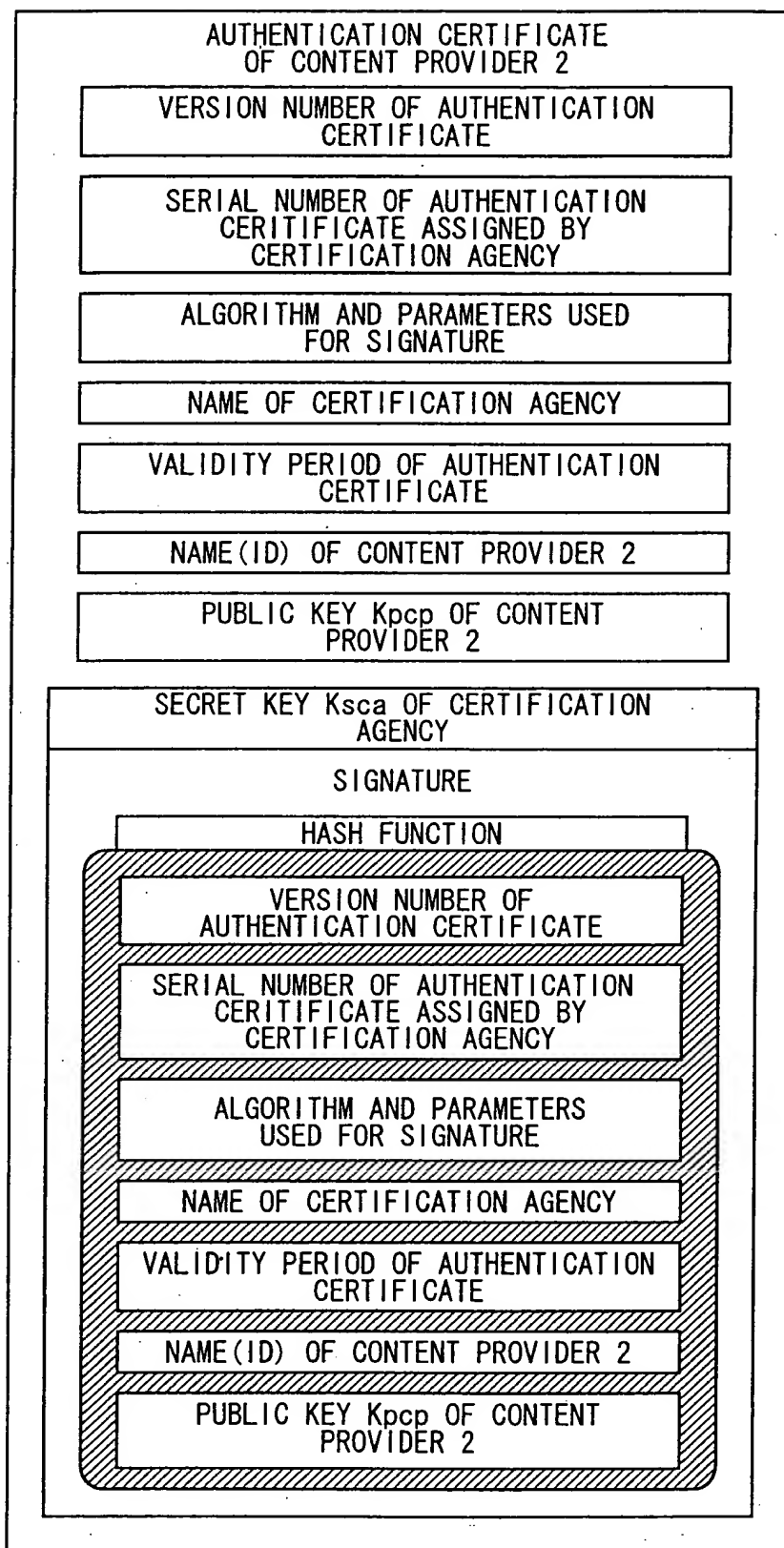
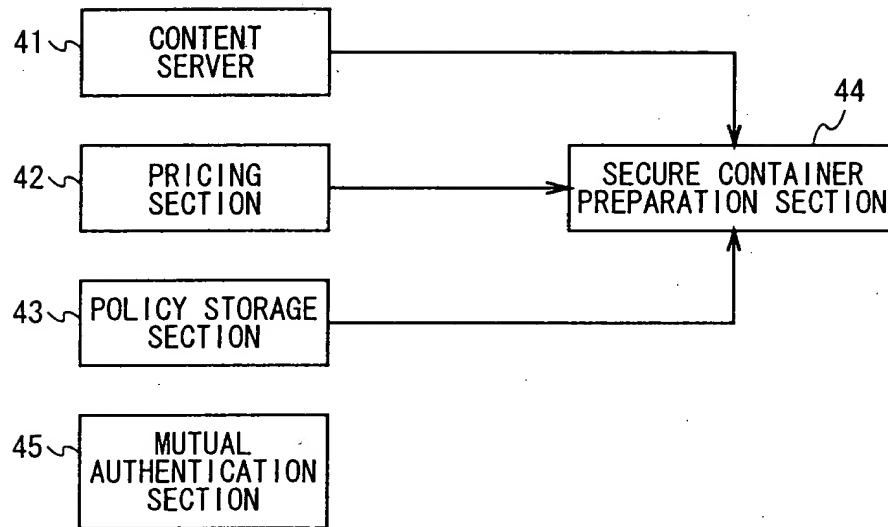


FIG. 14



SERVICE PROVIDER 3

FIG. 15

CONTENT ID	ID OF CONTENT A	
CONTENT PROVIDER ID	ID OF CONTENT PROVIDER 2	
UCP ID	ID OF ucp A	
SERVICE PROVIDER ID	ID OF SERVICE PROVIDER 3	
PT ID	ID OF pTA-1	
PT VALIDITY PERIOD	VALIDITY PERIOD OF pTA-1	
PRICING CONDITIONS 10	USER CONDITIONS 10	MALE
	EQUIPMENT CONDITIONS 10	NO CONDITIONS
PRICE 11	2000YEN	
PRICE 12	600YEN	
PRICE 13	100YEN	
PRICE 14	300YEN	
PRICE 15	1950YEN	
PRICE 16	1000YEN	

(B)

CONTENT ID	ID OF CONTENT A	
CONTENT PROVIDER ID	ID OF CONTENT PROVIDER 2	
UCP ID	ID OF ucp A	
SERVICE PROVIDER ID	ID OF SERVICE PROVIDER 3	
PT ID	ID OF pTA-2	
PT VALIDITY PERIOD	VALIDITY PERIOD OF pTA-2	
PRICING CONDITIONS 20	USER CONDITIONS 20	FEMALE
	EQUIPMENT CONDITIONS 20	NO CONDITIONS
PRICE 21	1000YEN	
PRICE 22	300YEN	
PRICE 23	50YEN	
PRICE 24	150YEN	
PRICE 25	1980YEN	
PRICE 26	500YEN	

FIG. 16

SECRET

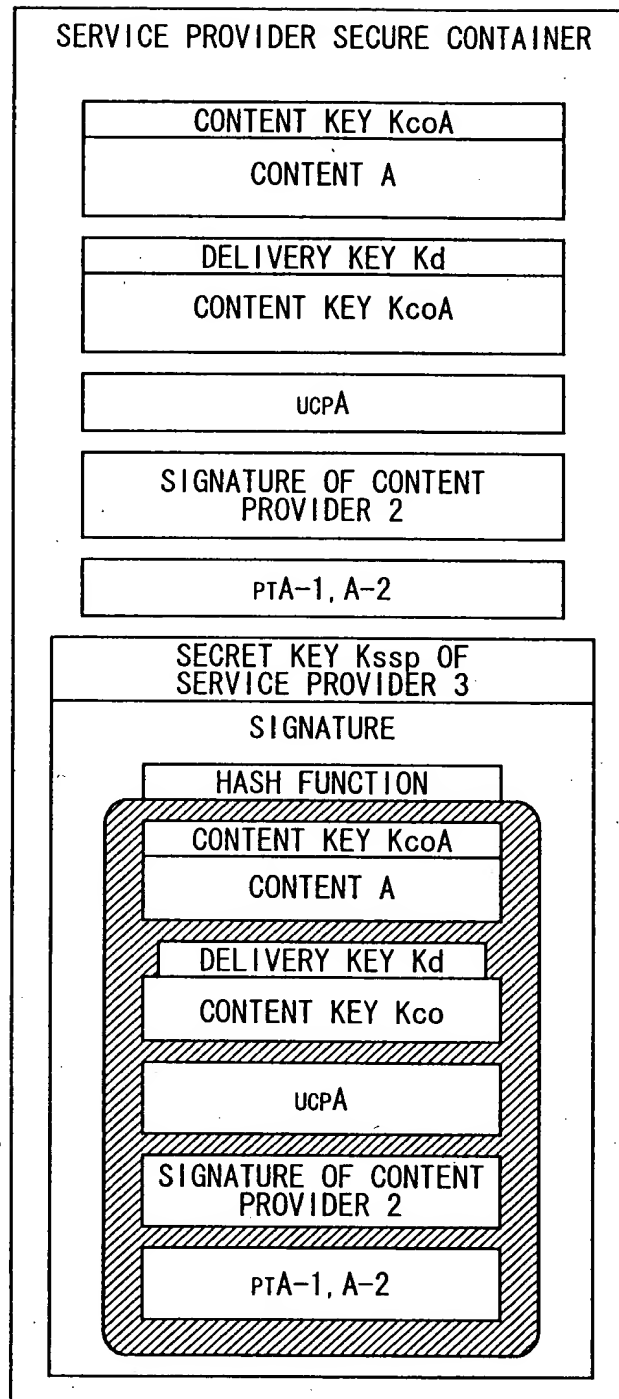


FIG. 17

09/719056 0000 0000 0000 0000 0000 0000

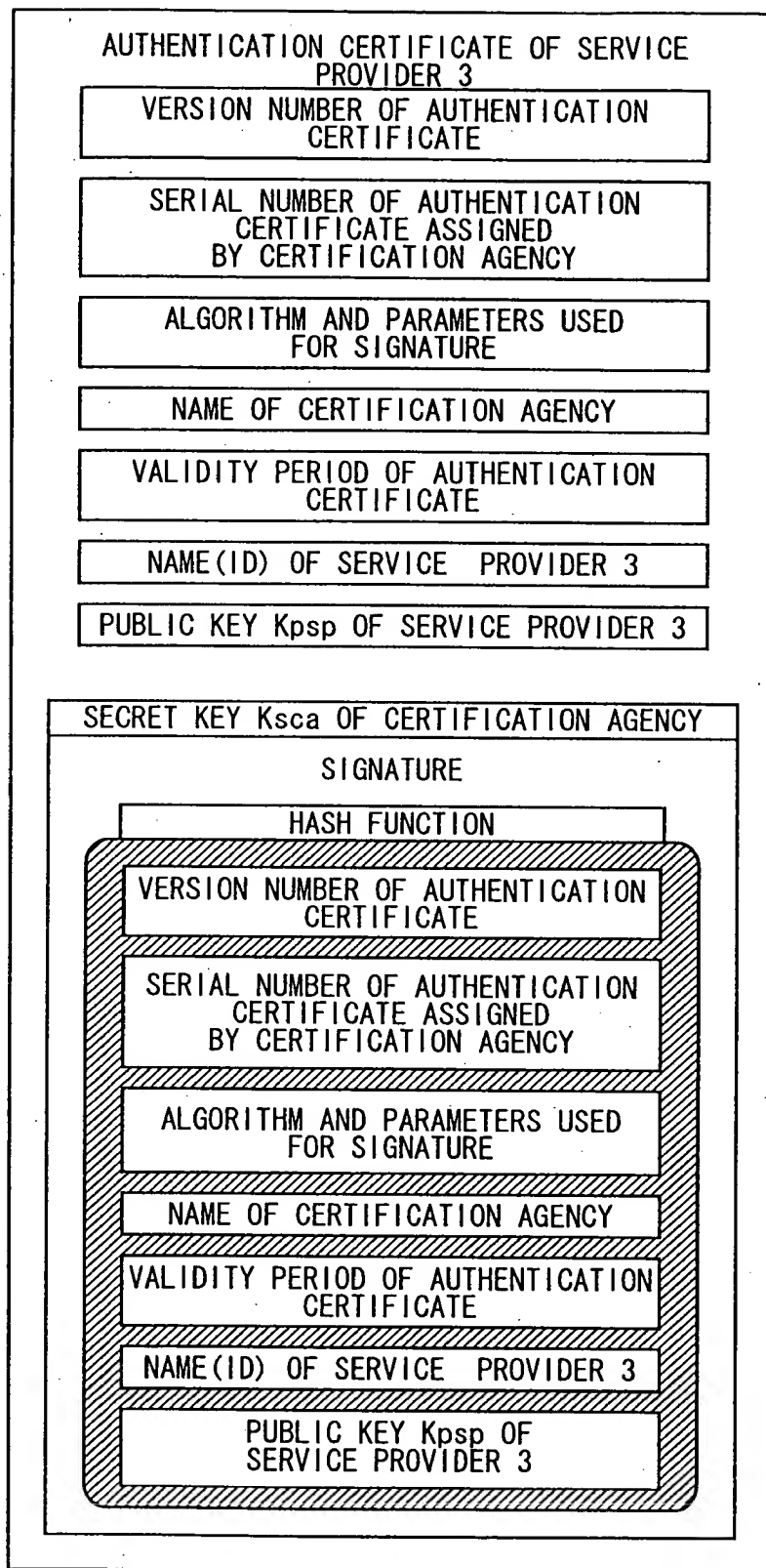
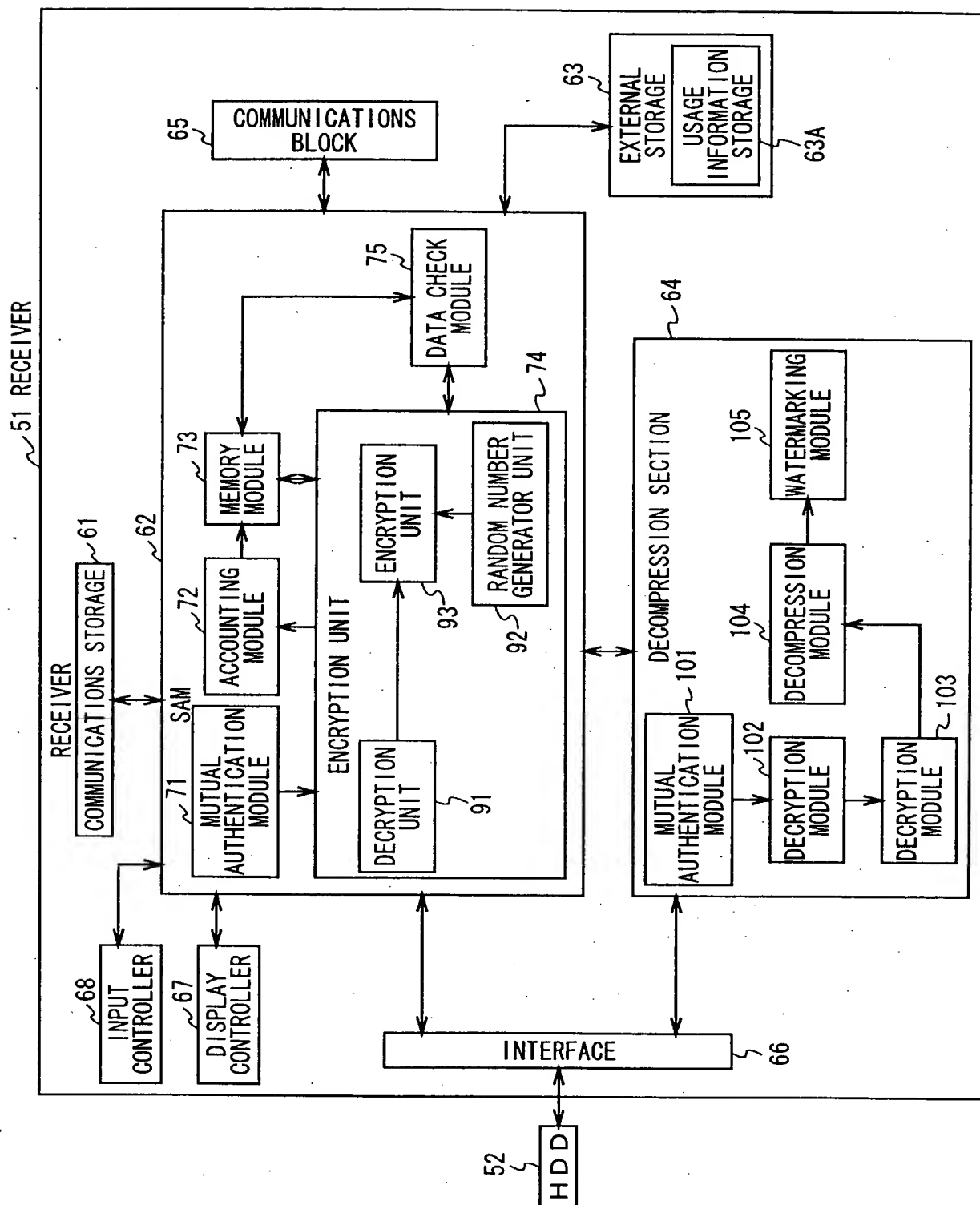


FIG. 18



09/719056

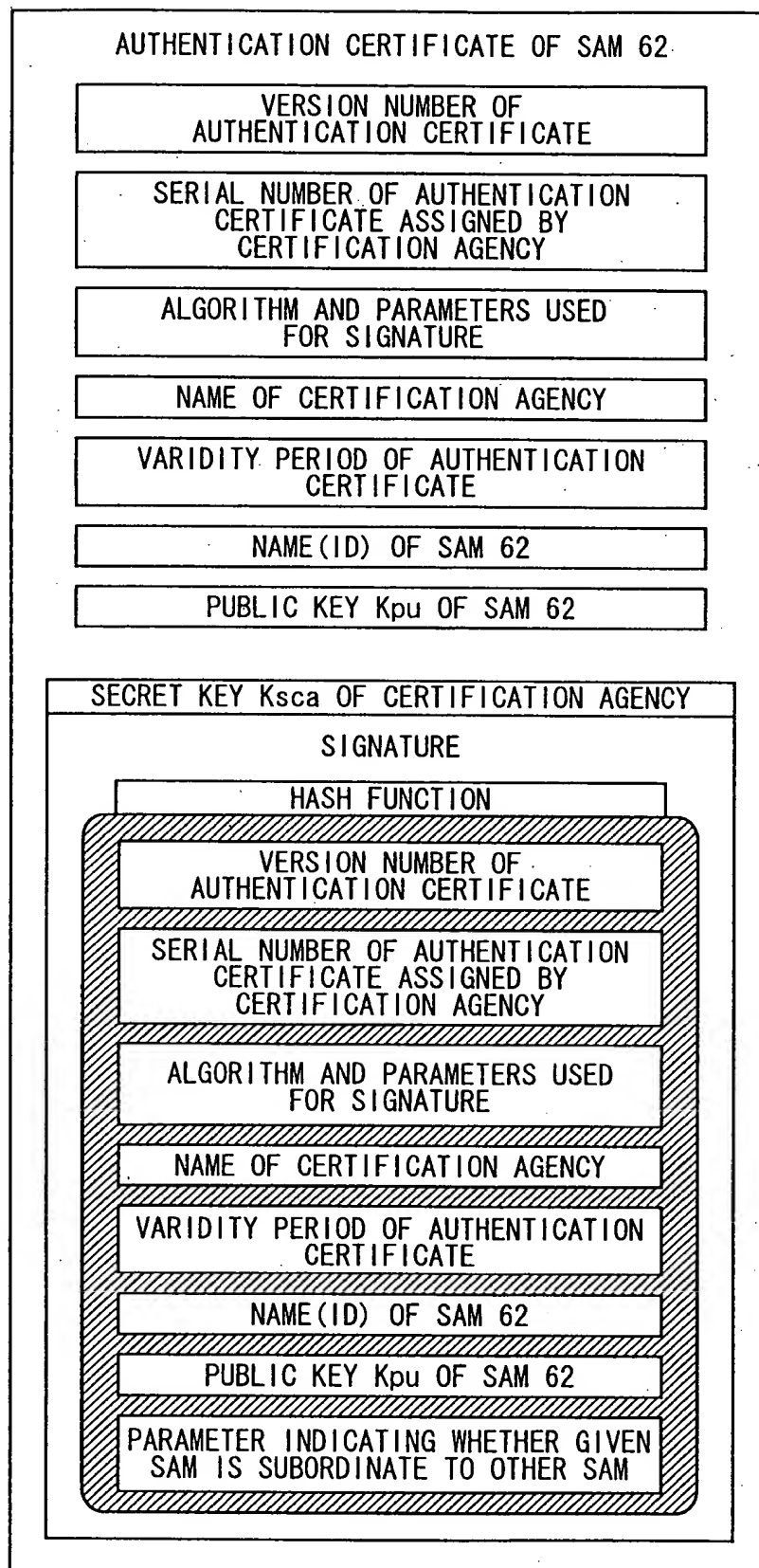


FIG. 20

UCSA

21/53

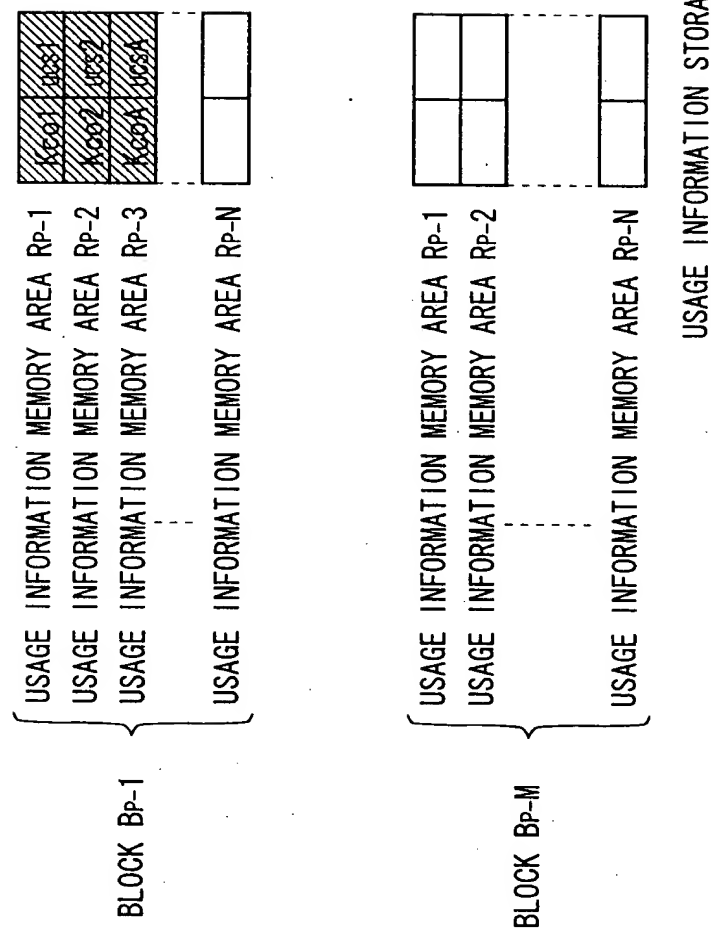


FIG. 22

CONTENT ID	ID OF CONTENT A
CONTENT PROVIDER ID	ID OF CONTENT PROVIDER 2
UCP ID	ID OF UCPA
UCP VALIDITY PERIOD	VALIDITY PERIOD OF UCPA
SERVICE PROVIDER ID	ID OF SERVICE PROVIDER 3
PT ID	ID OF PTA-1
PT VALIDITY PERIOD	VALIDITY PERIOD OF PTA-1
UCS ID	ID OF UCSA
SAM ID	ID OF SAM62
USER ID	ID OF USER F
USAGE DETAILS	ID
	ID OF USAGE DETAILS 13
	TYPE
	LIMITED-TIME REPRODUCTION
	PARAMETER
	× × ×
	CONTROL TRANSFER STATUS
	SOURCE: ID OF SAM62, DESTINATION: ID OF SAM62

ACCOUNTING INFORMATION A

FIG. 23

PUBLIC KEY K_{pu} OF SAM62		
SECRET KEY K_{su} OF SAM62		
PUBLIC KEY K_{pesc} OF THE EMD SERVICE CENTER 1		
PUBLIC KEY K_{pca} OF THE CERTIFICATION AGENCY		
SAVE KEY K_{save}		
THREE MONTHS' DELIVERY KEYS K_d		
⋮		
AUTHENTICATION CERTIFICATE OF SAM62		
REFERENCE INFORMATION 51		
ACCOUNTING INFORMATION		
⋮		
VERIFICATION VALUES H_{p-1}	VERIFICATION VALUES H_{p-2}
.....		VERIFICATION VALUES H_{p-M}

FIG. 24

•

FIG. 25

LIST SECTION

SAM ID	USER ID	PURCHASING	ACCOUNTING	EQUIPMENT BILLED	MASTER EQUIPMENT	STATUS FLAG	SIGNATURE TO CONDITIONS	SIGNATURE TO REGISTRATION LIST
ID OF SAM62	USER ID OF USER F	YES	YES	ID OF SAM62	NONE	NO RESTRICTION	x x x x	x x x x
ID OF SAM212	USER ID OF USER F	YES	YES	ID OF SAM212	ID OF SAM62	NO RESTRICTION	x x x x	
ID OF SAM312	USER ID OF USER F	NO	NO	NONE	ID OF SAM62	NO RESTRICTION	x x x x	

REGISTRATION
CONDITIONS
OF RECEIVER 51

REGISTRATION
CONDITIONS
OF RECEIVER 201

REGISTRATION
CONDITIONS
OF RECEIVER 301

SAM ID: ID OF SAM62	ID OF SAM62
VALIDITY PERIOD	x x x x
VERSION NUMBER	x x x x
NUMBER OF EQUIPMENT CONNECTED	3

SAM INFORMATION SECTION

FIG. 26

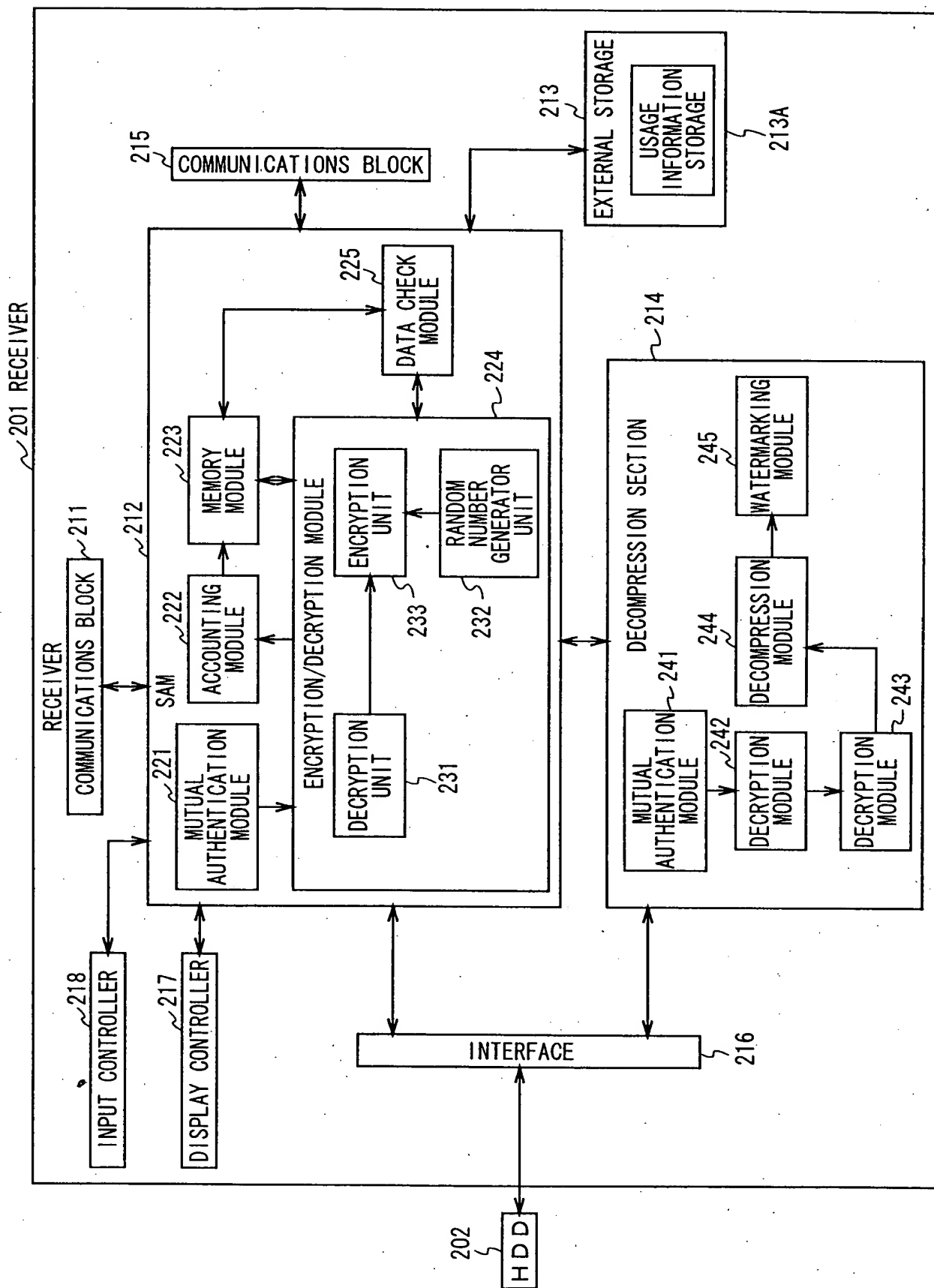


FIG. 27

SAM ID		ID OF SAM212
EQUIPMENT NUMBER		EQUIPMENT NUMBER(100) OF RECEIVERS 201
SETTLEMENT ID		SETTLEMENT ID OF USER F
CHARGE LIMIT		FORMAL REGISTRATION
ACCOUNT-SETTLING USER INFORMATION	NAME	NAME OF USER F
	ADDRESS	ADDRESS OF USER F
	PHONE NUMBER	PHONE NUMBER OF USER F
	SETTLEMENT INSTITUTION INFORMATION	SETTLEMENT INSTITUTION INFORMATION OF USER F
	DATE OF BIRTH	DATA OF BIRTH OF USER F
	AGE	AGE OF USER F
	SEX	SEX OF USER F
	USER ID	USER ID OF USER F
	PASSWORD	PASSWORD OF USER F
SUBORDINATE USER INFORMATION	NAME	NAME OF USER A
	ADDRESS	ADDRESS OF USER A
	PHONE NUMBER	PHONE NUMBER OF USER A
	DATE OF BIRTH	DATA OF BIRTH OF USER A
	SEX	SEX OF USER A
	USER ID	USER ID OF USER A
	PASSWORD	PASSWORD OF USER A
USE POINT INFORMATION		USE POINT INFORMATION OF RECEIVERS 201

REFERENCE INFORMATION 201

FIG. 28

LIST SECTION

SAM ID	USER ID	PURCH- ASING	ACCOU- NTING	EQUIPMENT	MASTER EQUIPMENT	STATUS FLAG	SIGNATURE TO CONDITIONS	SIGNATURE TO REGISTRATION LIST
ID OF SAM62	USER ID OF USER F	YES	YES	ID OF SAM62	NONE	NO RESTRICTION	x x x x	x x x x
ID OF SAM212	USER ID OF USER F	YES	YES	ID OF SAM212	ID OF SAM62	NO RESTRICTION	x x x x	

REGISTRATION
CONDITIONS OF
RECEIVER 51

REGISTRATION
CONDITIONS OF
RECEIVER 201

SAM ID	ID OF SAM212
VALIDITY PERIOD	x x x x
VERSION NUMBER	x x x x
NUMBER OF EQUIPMENT CONNECTED	2

SAM INFORMATION SECTION

FIG. 29

301 RECEIVER

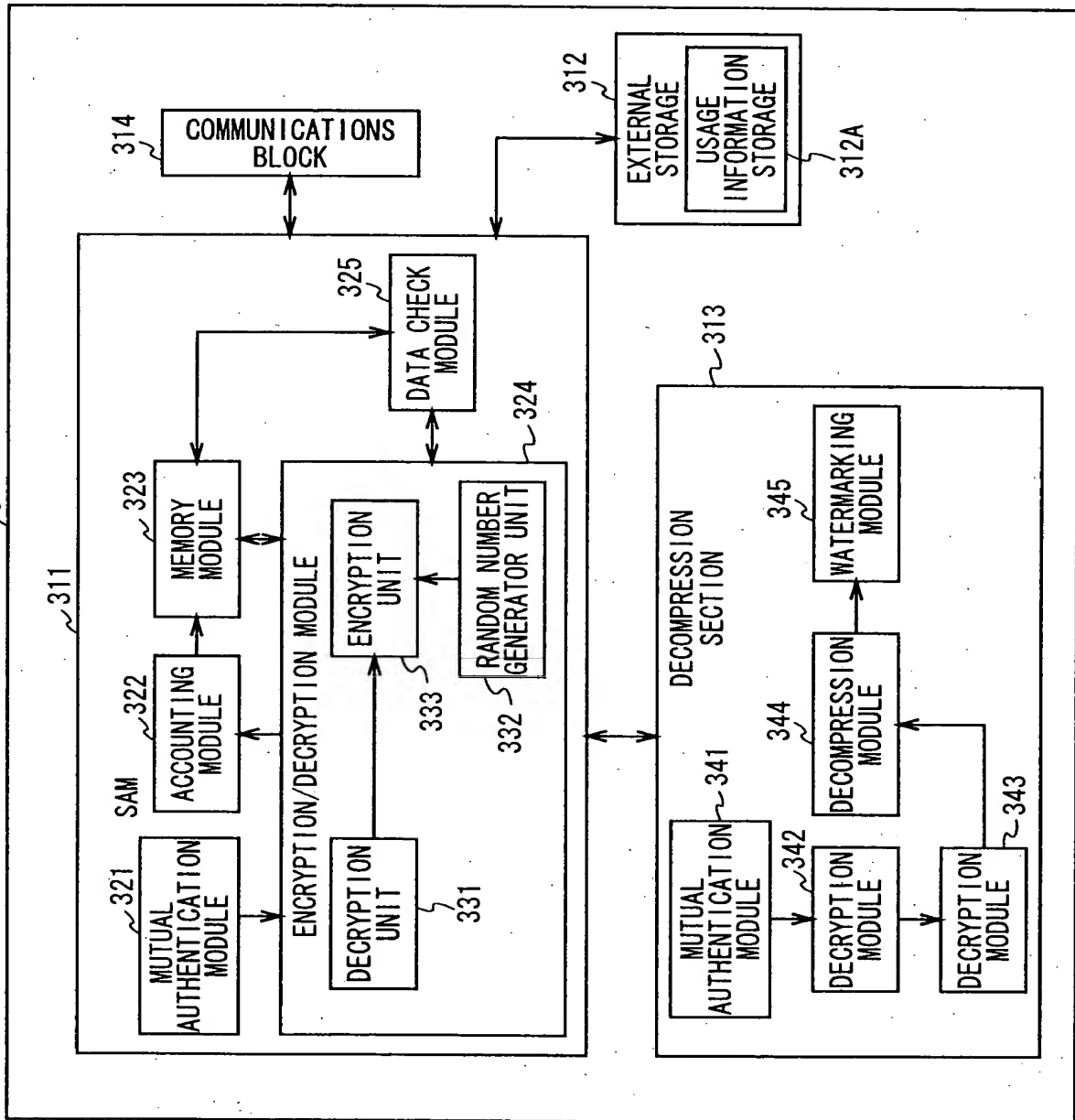


FIG. 30

SAM ID		ID OF SAM311
EQUIPMENT NUMBER		EQUIPMENT NUMBER(25) OF RECEIVERS 301
SETTLEMENT ID		SETTLEMENT ID OF USER F
CHARGE LIMIT		FORMAL REGISTRATION
ACCOUNT-SETTLING USER INFORMATION	NAME	NAME OF USER F
	ADDRESS	ADDRESS OF USER F
	PHONE NUMBER	PHONE NUMBER OF USER F
	SETTLEMENT INSTITUTION INFORMATION	SETTLEMENT INSTITUTION INFORMATION OF USER F
	DATE OF BIRTH	DATA OF BIRTH OF USER F
	AGE	AGE OF USER F
	SEX	SEX OF USER F
	USER ID	USER ID OF USER F
	PASSWORD	PASSWORD OF USER F
SUBORDINATE USER INFORMATION	NAME	NAME OF USER A
	ADDRESS	ADDRESS OF USER A
	PHONE NUMBER	PHONE NUMBER OF USER A
	DATE OF BIRTH	DATA OF BIRTH OF USER A
	SEX	SEX OF USER A
	USER ID	USER ID OF USER A
	PASSWORD	PASSWORD OF USER A
USE POINT INFORMATION		USE POINT INFORMATION OF RECEIVERS 301

REFERENCE INFORMATION 301

FIG. 31

LIST SECTION

SAM ID	USER ID	PURCH- ASING	ACCOU- NTING	EQUIPMENT BILLED	MASTER EQUIPMENT	STATUS FLAG
ID OF SAM311	USER ID OF USER F	NO	NO	NONE	ID OF SAM62	NO RESTRICTION

REGISTRATION
CONDITIONS OF
RECEIVER 301

SAM ID	ID OF SAM311
VALIDITY PERIOD	x x x x
VERSION NUMBER	x x x x
NUMBER OF EQUIPMENT CONNECTED	2

SAM INFORMATION SECTION

FIG. 32

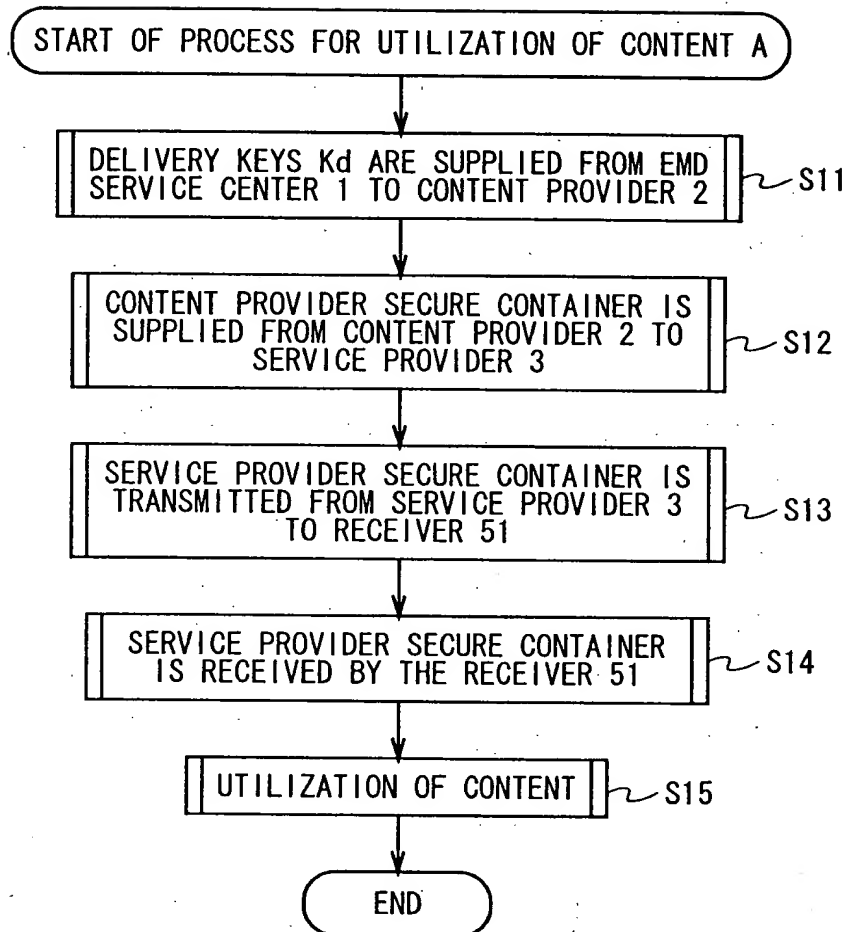


FIG. 33

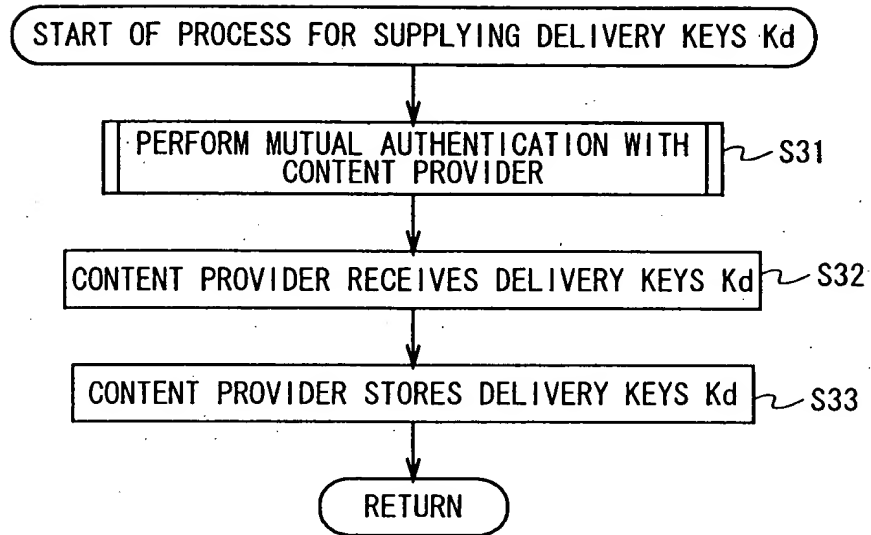


FIG. 34

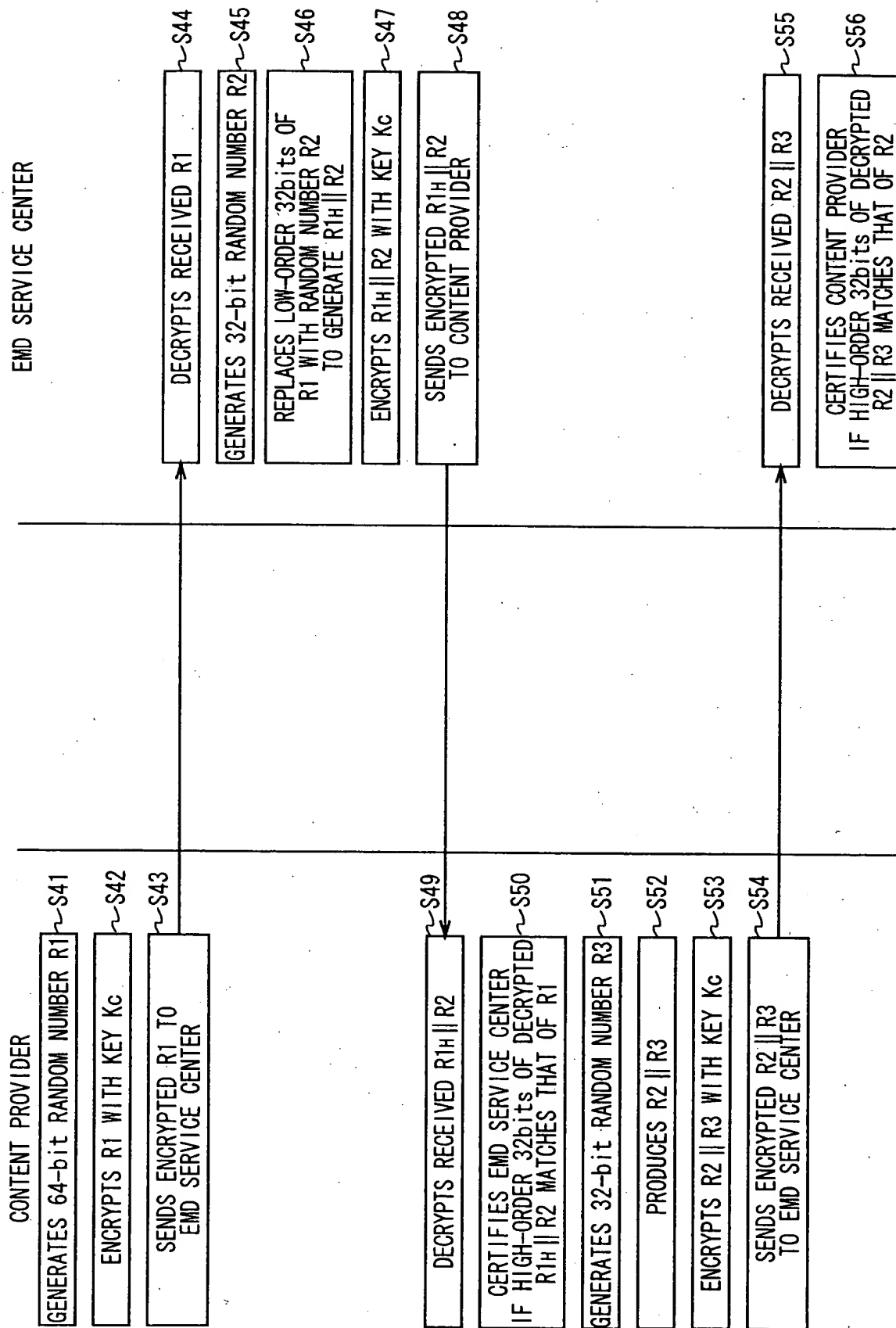


FIG. 35

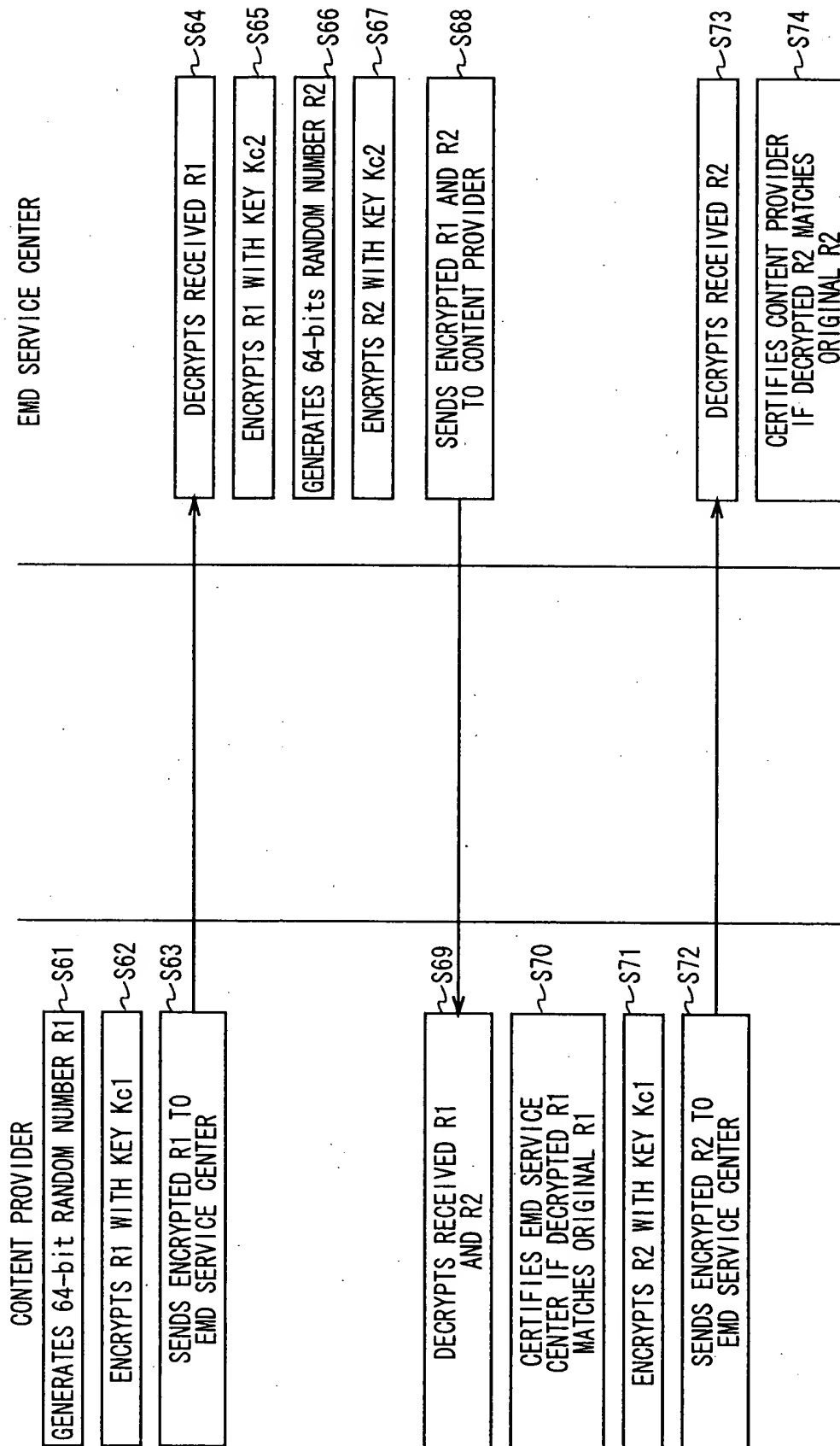


FIG. 36

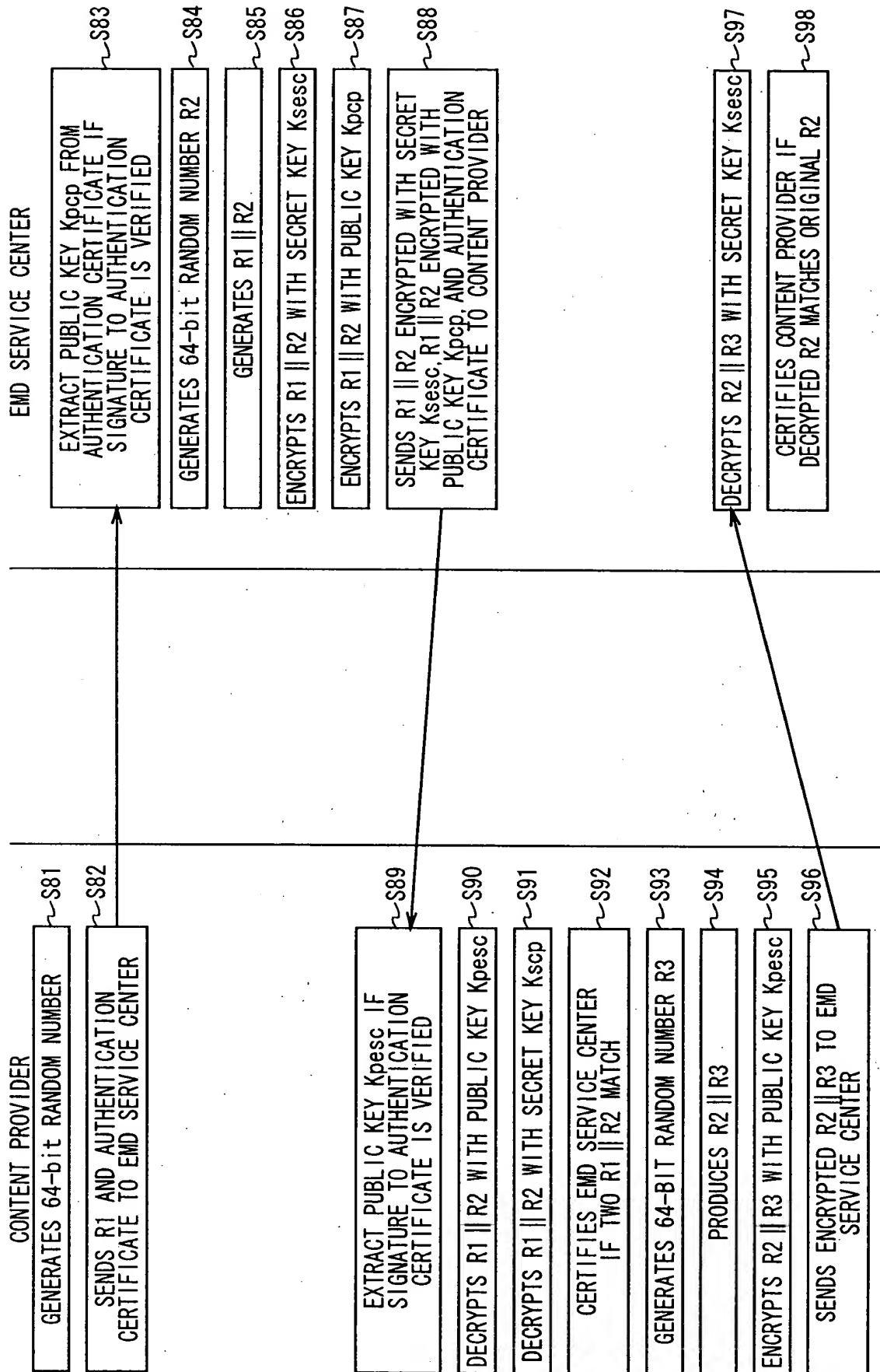


FIG. 37

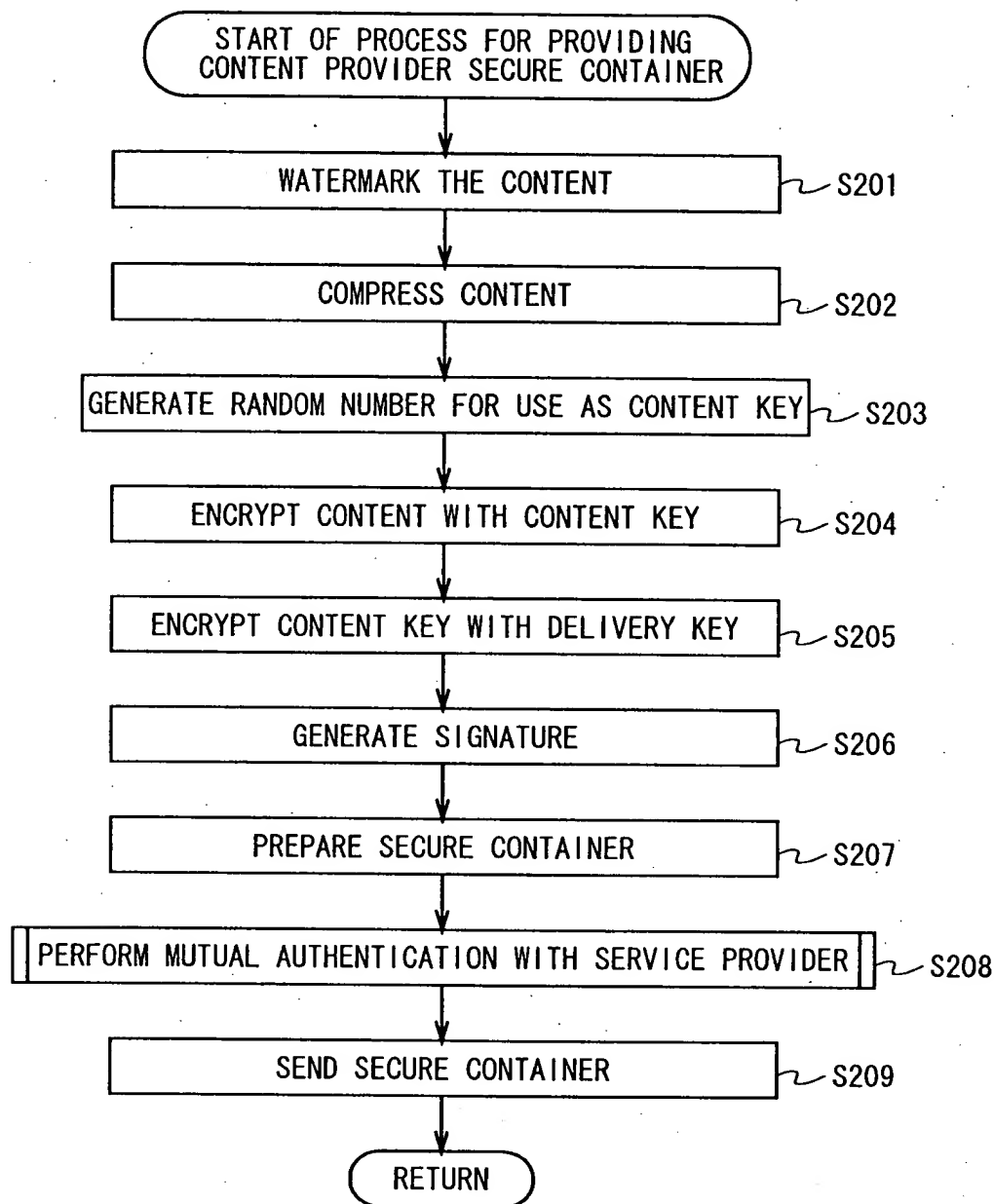


FIG. 38

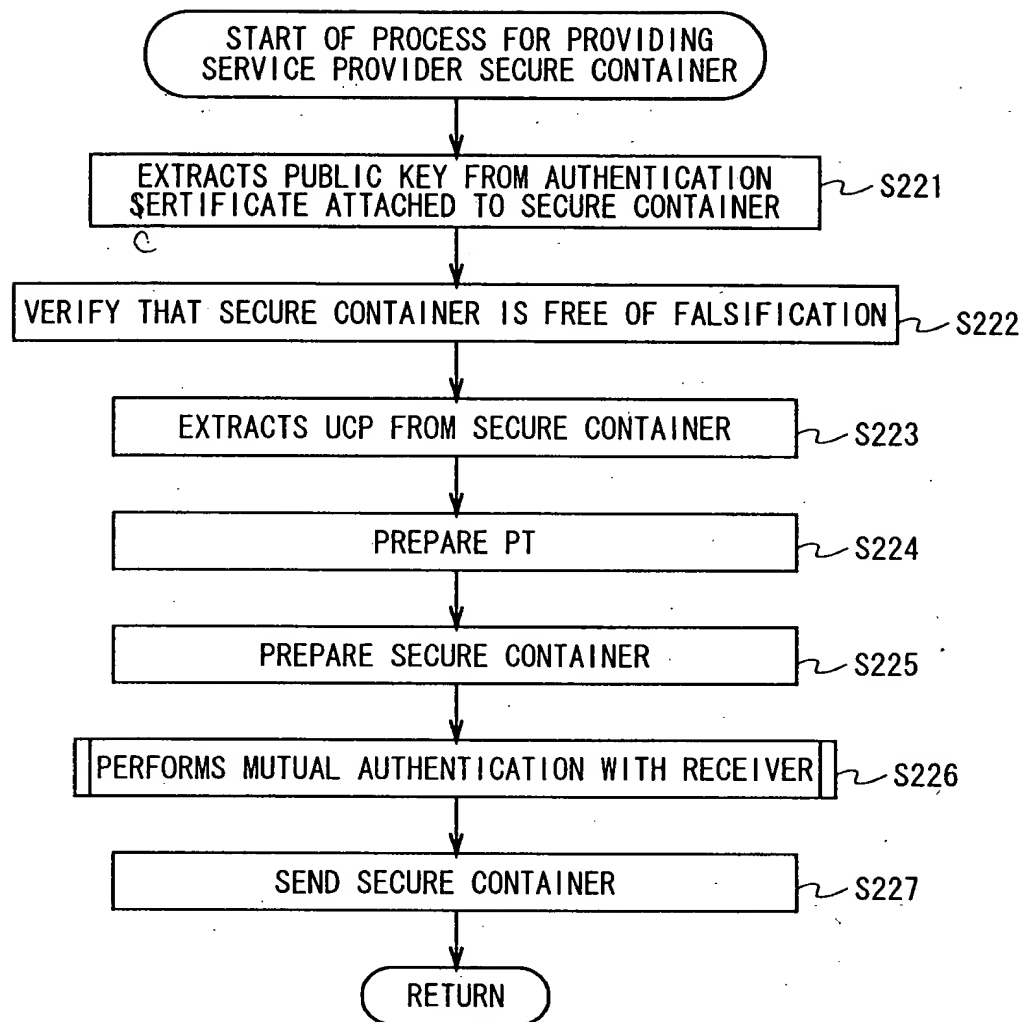


FIG. 39

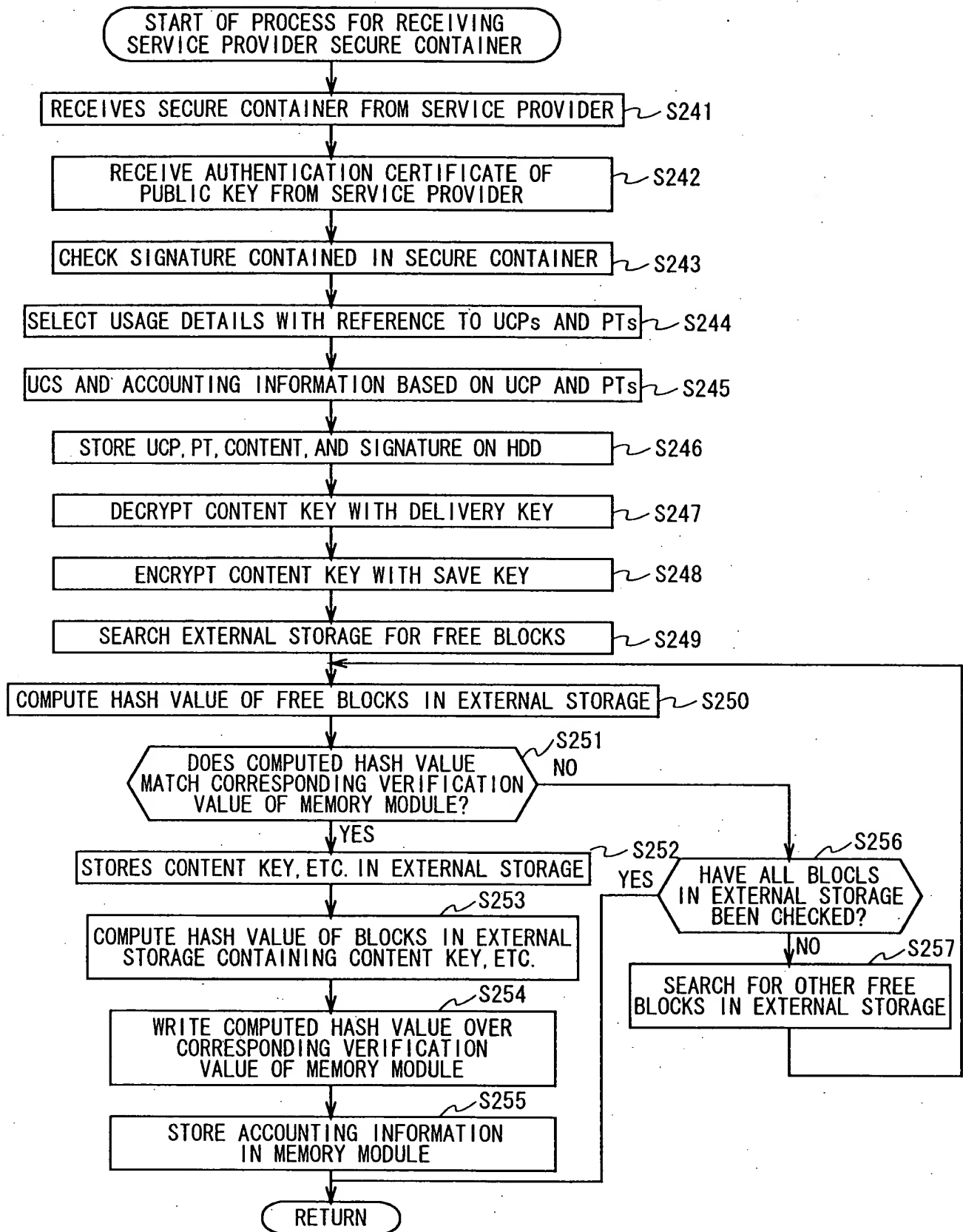


FIG. 40

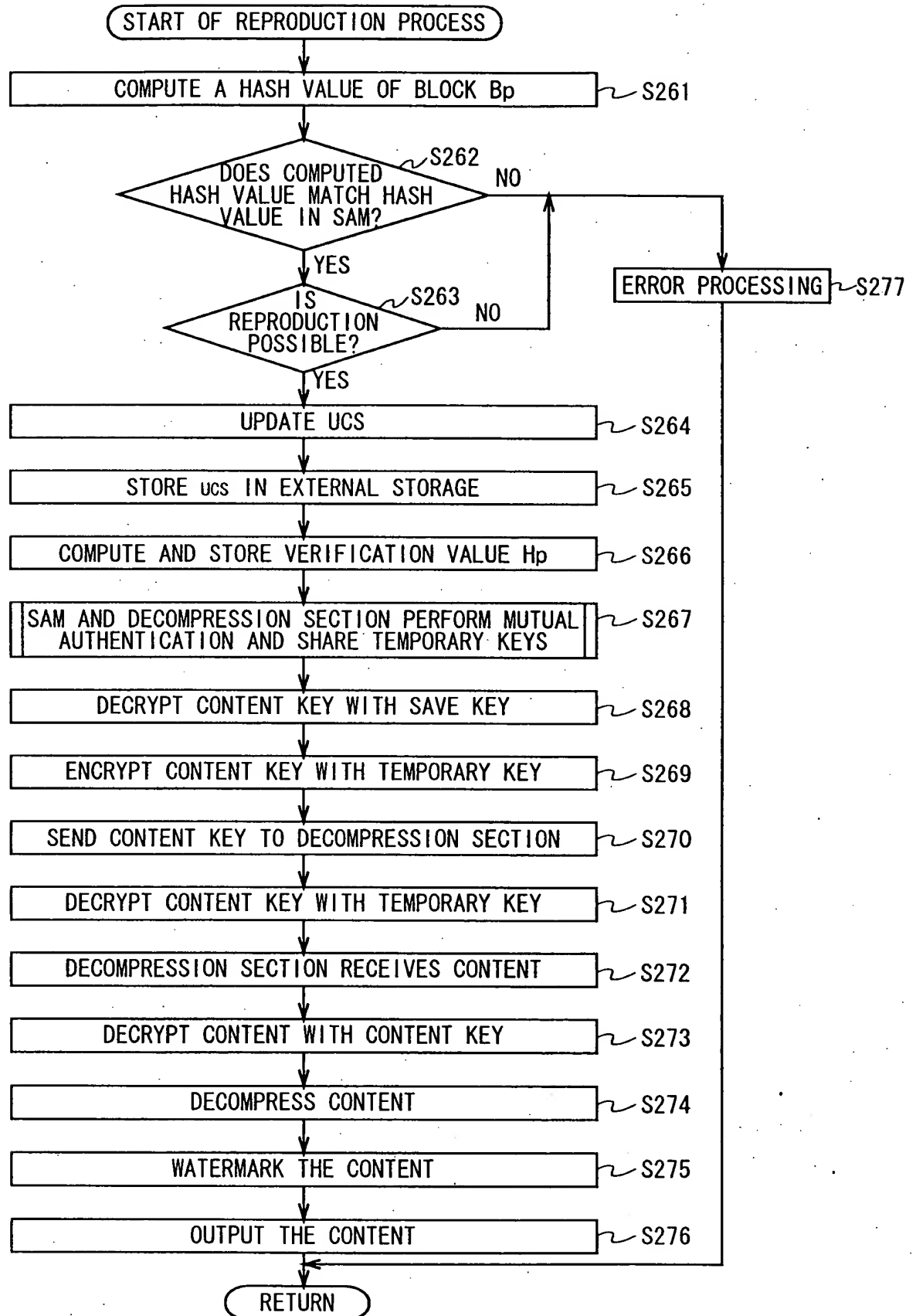


FIG. 41
41/53

019056 019056 019056

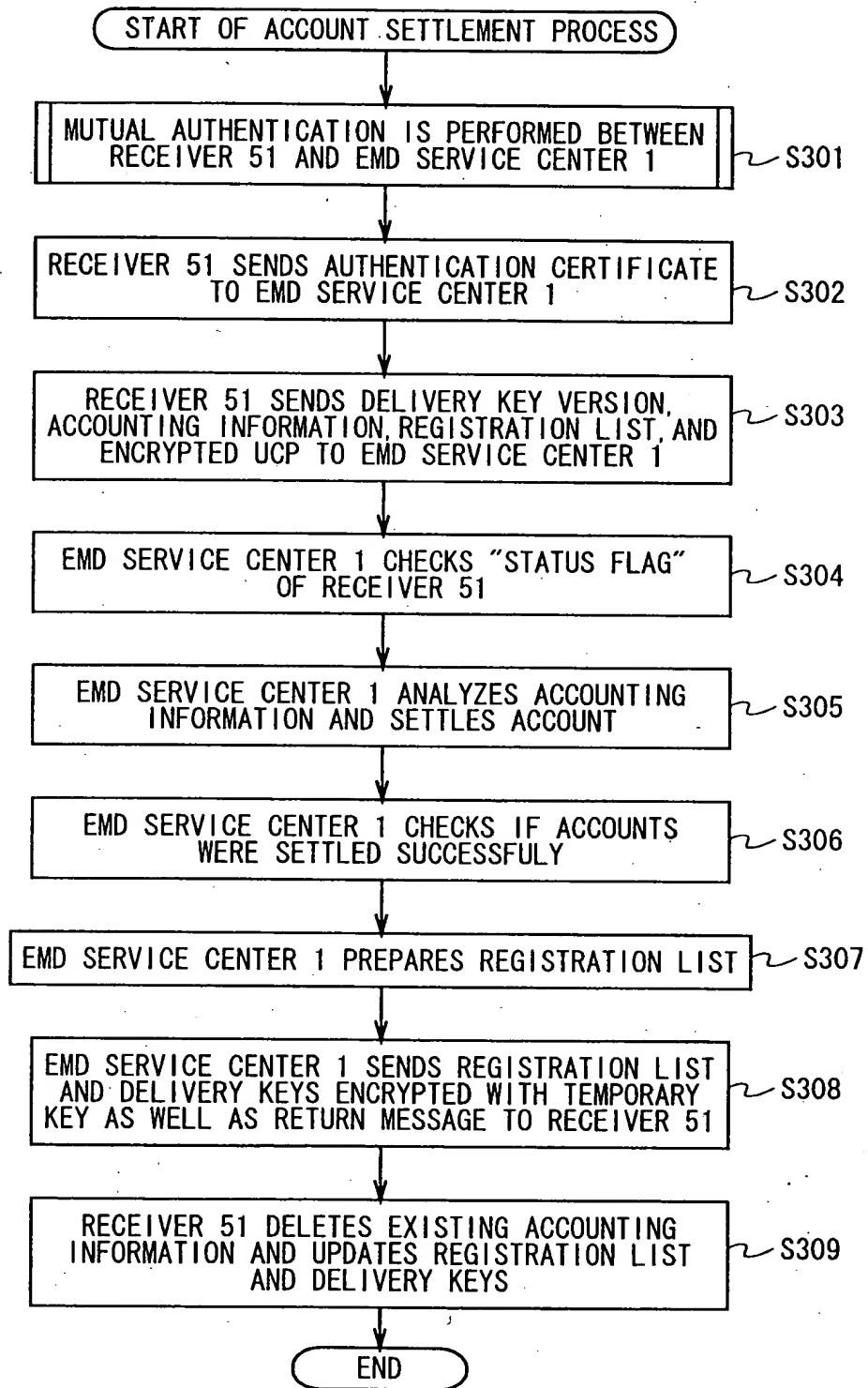


FIG. 42

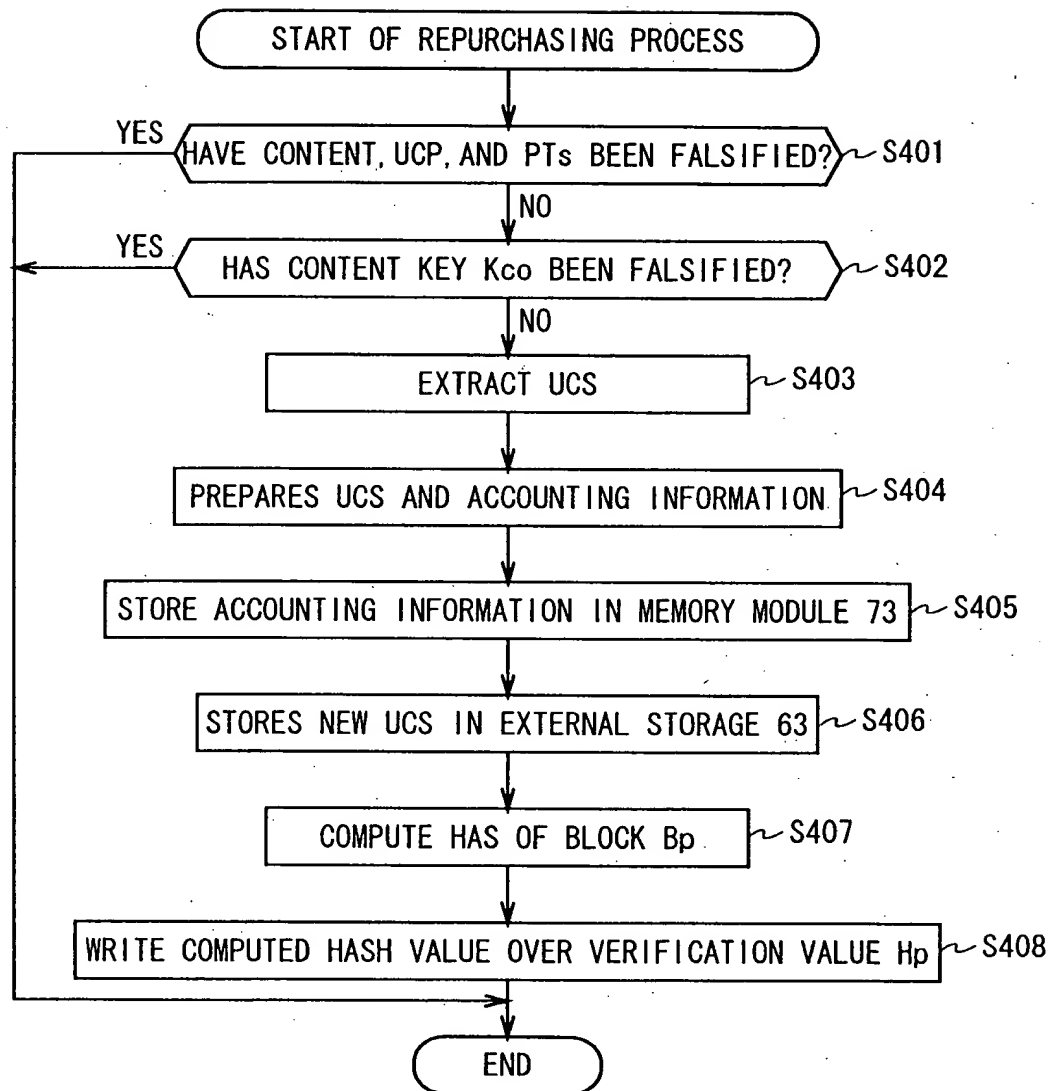


FIG. 43

CONTENT ID	ID OF CONTENT A
CONTENT PROVIDER ID	ID OF CONTENT PROVIDER 2
UCP ID	ID OF ucpA
UCP VALIDITY PERIOD	VALIDITY PERIOD OF ucpA
SERVICE PROVIDER ID	ID OF SERVICE PROVIDER 3
PT ID	ID OF pTA-1
PT VALIDITY PERIOD	VALIDITY PERIOD OF pTA-1
UCS ID	ID OF ucsA
SAM ID	ID OF SAM62
USER ID	ID OF USER F
USAGE DETAILS	ID
	TYPE
	PARAMETER
	CONTROL TRANSFER STATUS
SOURCE: ID OF SAM62 DESTINATION: ID OF SAM62	
USAGE HISTORY	x x x

ucsB

FIG. 44

CONTENT ID	ID OF CONTENT A
CONTENT PROVIDER ID	ID OF CONTENT PROVIDER 2
UCP ID	ID OF uCPA
UCP VALIDITY PERIOD	VALIDITY PERIOD OF uCPA
SERVICE PROVIDER ID	ID OF SERVICE PROVIDER 3
PT ID	ID OF pTA-1
PT VALIDITY PERIOD	VALIDITY PERIOD OF pTA-1
UCS ID	ID OF uCSA
SAM ID	ID OF SAM62
USER ID	ID OF USER F
USAGE DETAILS	ID
	TYPE
	PARAMETER
	CONTROL TRANSFER STATUS
	ID OF USAGE DETAILS 15
	TYPE13→TYPE 11
	x x x
	SOURCE: ID OF SAM62 DESTINATION: ID OF SAM62

ACCOUNTING INFORMATION B

FIG. 45

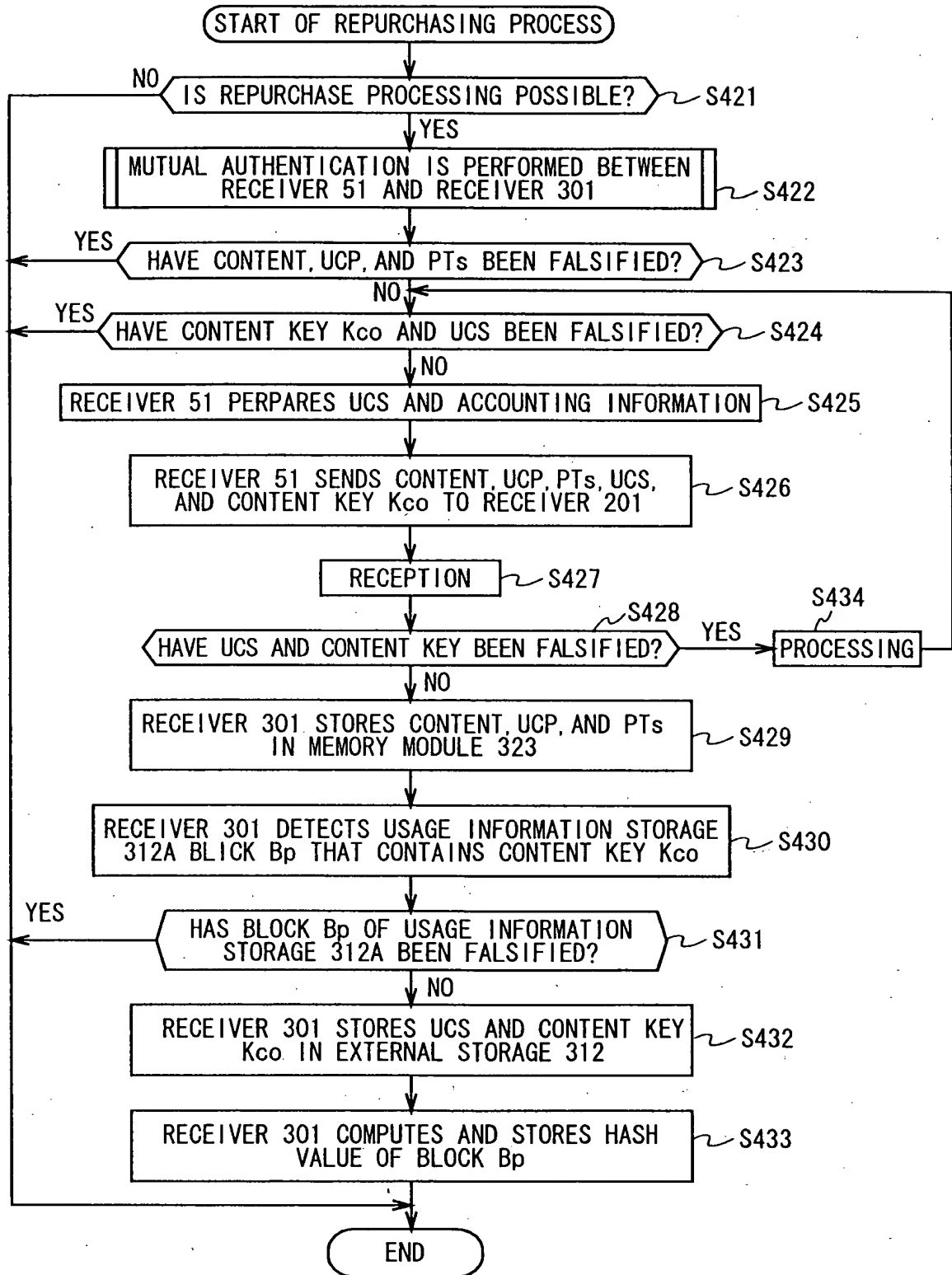


FIG. 46

CONTENT ID	ID OF CONTENT A
CONTENT PROVIDER ID	ID OF CONTENT PROVIDER 2
UCP ID	ID OF uCPA
UCP VALIDITY PERIOD	VALIDITY PERIOD OF uCPA
SERVICE PROVIDER ID	ID OF SERVICE PROVIDER 3
PT ID	ID OF pTA-1
PT VALIDITY PERIOD	VALIDITY PERIOD OF pTA-1
UCS ID	ID OF uCSA
SAM ID	ID OF SAM62
USER ID	ID OF USER F
USAGE DETAILS	ID
	TYPE
	PARAMETER
	CONTROL TRANSFER STATUS
SOURCE: ID OF SAM62 DESTINATION: ID OF SAM62	
USAGE HISTORY	

uCS

FIG. 47

09719056:0971904

CONTENT ID	ID OF CONTENT A
CONTENT PROVIDER ID	ID OF CONTENT PROVIDER 2
UCP ID	ID OF uCPA
UCP VALIDITY PERIOD	VALIDITY PERIOD OF uCPA
SERVICE PROVIDER ID	ID OF SERVICE PROVIDER 3
PT ID	ID OF pTA-1,
PT VALIDITY PERIOD	VALIDITY PERIOD OF pTA-1
UCS ID	ID OF ucsA
SAM ID	ID OF SAM62
USER ID	ID OF USER F
USAGE DETAILS	ID
	ID OF USAGE DETAILS 16
	TYPE
	TYPE 11→TYPE 11
CONTROL TRANSFER STATUS	PARAMETER
	× × ×
SOURCE: ID OF SAM62 DESTINATION: ID OF SAM62	

ACCOUNTING INFORMATION C

FIG. 48

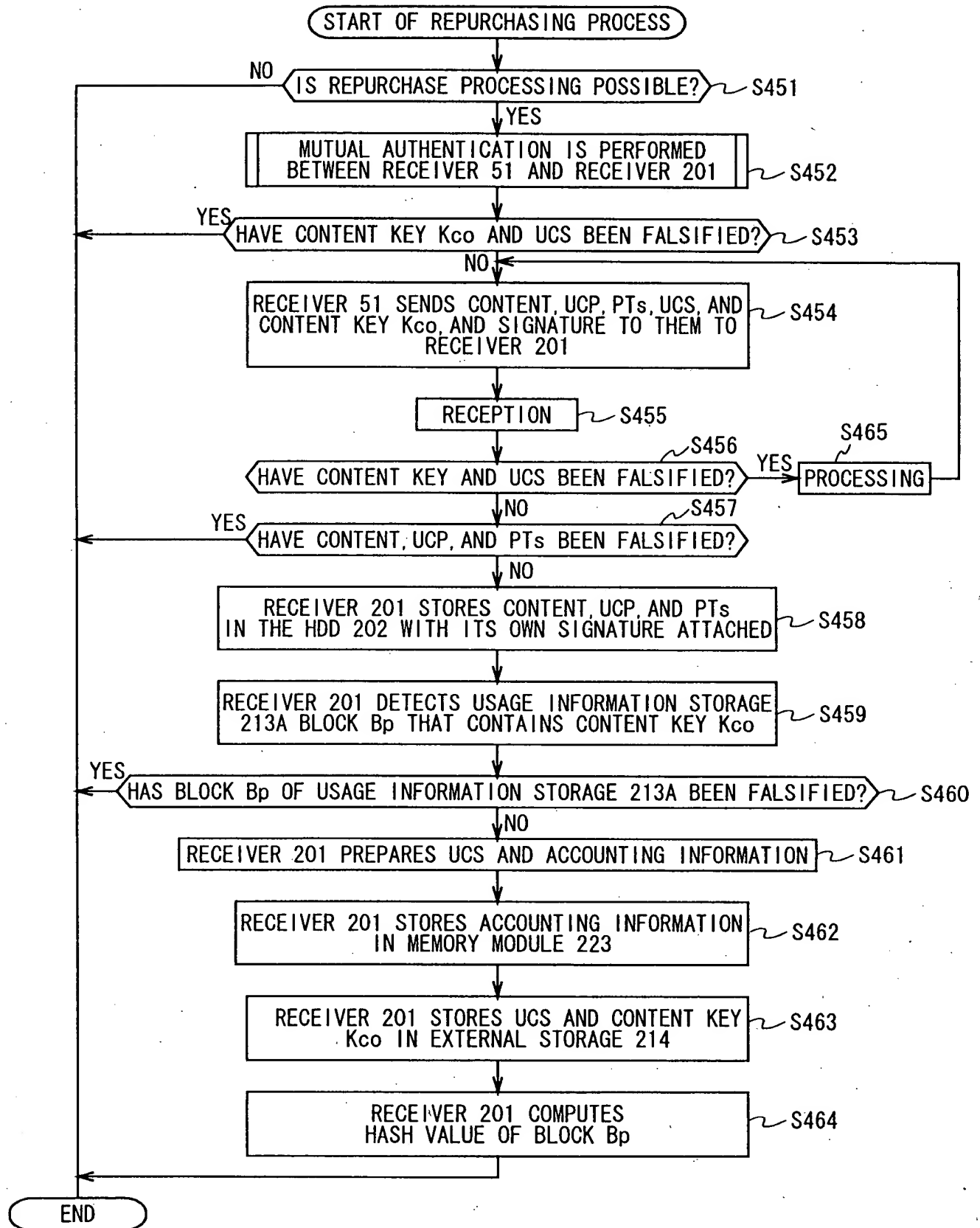


FIG. 49

CONTENT ID	ID OF CONTENT A
CONTENT PROVIDER ID	ID OF CONTENT PROVIDER 2
UCP ID	ID OF uCPA
UCP VALIDITY PERIOD	VALIDITY PERIOD OF uCPA
SERVICE PROVIDER ID	ID OF SERVICE PROVIDER 3
PT ID	ID OF pTA-1
PT VALIDITY PERIOD	VALIDITY PERIOD OF pTA-1
UCS ID	ID OF ucsA
SAM ID	ID OF SAM212
USER ID	ID OF USER F
USAGE DETAILS	ID
	TYPE
	PARAMETER
	CONTROL TRANSFER STATUS
SOURCE: ID OF SAM62 DESTINATION: ID OF SAM62	
USAGE HISTORY	x x x

ucsD

FIG. 50

CONTENT ID	ID OF CONTENT A
CONTENT PROVIDER ID	ID OF CONTENT PROVIDER 2
UCP ID	ID OF uCPA
UCP VALIDITY PERIOD	VALIDITY PERIOD OF uCPA
SERVICE PROVIDER ID	ID OF SERVICE PROVIDER 3
PT ID	ID OF pTA-1
PT VALIDITY PERIOD	VALIDITY PERIOD OF pTA-1
UCS ID	ucsAのID
SAM ID	ID OF SAM212
USER ID	ID OF USER F
USAGE DETAILS	ID
	TYPE
	PARAMETER
	CONTROL TRANSFER STATUS
	ID OF USAGE DETAILS 16
	TYPE 11→TYPE 11
	× × ×
	SOURCE: ID OF SAM62 DESTINATION: ID OF SAM62

ACCOUNTING INFORMATION D

FIG. 51

Explanation of Reference Numerals

1 ... EMD service center, 2 ... content provider, 3 ... service provider, 5 ... user home network, 11 ... service provider management section, 12 ... content provider management section, 13 ... copyright management section, 14 ... key server, 15 ... log data management section, 16 ... profit-sharing section, 17 ... mutual authentication section, 18 ... user management section, 19 ... billing section, 20 ... cashier section, 21 ... audit section, 31 ... content server, 32 ... watermarking section, 33 ... compression section, 34 ... encryption section, 35 ... random number generator section, 36 ... encryption section, 37 ... policy storage section, 38 ... secure container preparation section, 39 ... mutual authentication section, 41 ... content server, 42 ... pricing section, 43 ... policy storage section, 44 ... secure container preparation section, 45 ... mutual authentication section, 51 ... receiver, 52 ... HDD, 61 ... communication block, 62 ... SAM, 63 ... external storage, 64 ... decompression section, 65 ... communication block, 66 ... interface, 67 ... display controller, 68 ... input controller, 71 ... mutual authentication module, 72 ... accounting module, 73 ... memory module, 74 ... encryption/decryption module, 75 ... data check module, 91 ... decryption unit, 92 ... random number generator unit, 93 ... encryption unit, 101 ... mutual authentication module, 102 ... decryption module, 103 ... decryption module, 104 ... decompression module, 105 ... watermarking module, 201 ... receiver, 202 ... HDD,

211 ... communication block, 212 ... SAM, 213 ... external storage,
 214 ... decompression section, 215 ... communication block, 216 ...
 interface, 217 ... display controller, 218 ... input controller, 221 ...
 mutual authentication module, 222 ... accounting module, 223 ... memory
 module, 224 ... encryption/decryption module, 225 ... data check module,
 231 ... decryption unit, 232 ... random number generator unit, 233 ...
 encryption unit, 241 ... mutual authentication module, 242 ...
 decryption module, 243 ... decryption module, 244 ... decompression
 module, 245 ... watermarking module.

09/719056